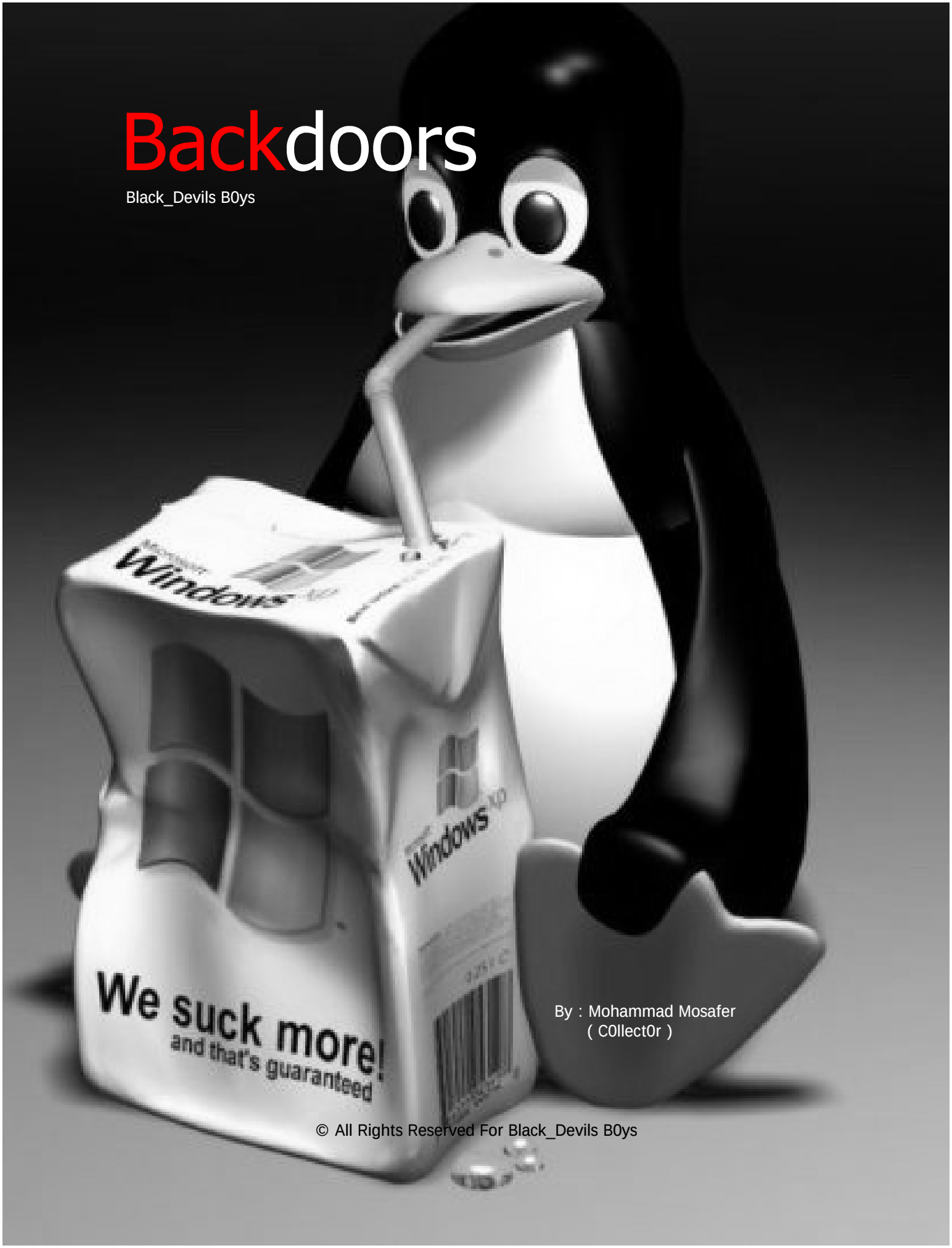
Backdoors

Black_Devils B0ys



By : Mohammad Mosafer
(C0llect0r)

به نام خدا

Black_Devils B0ys

پسران شیاطین سیاه

Backdoors

مباحثی پیرامون درهای پشتی

نویسنده : محمد مسافر (C0llect0r)

تاریخ : 2/3/2005

Contact

C0llect0r@SpYmAc.com
B0rn2h4k@YaHoO.com

Special TNX 2

P0fn0r- N0thing – Invisible.boy –Sp00f3r

White Journal

مقدمه :

در بسیاری از کتب مربوط به امنیت شبکه یا در بسیاری از مقالات و همچنین در مناظرات و جلسات هکری با اصطلاحی به نام در های پشتی سیستم ها (Backdoor) برخورد می نمایید جهت تبیین علمی این موضوع و دسترسی به اطلاعات پایه ای تر در این رابطه این مقاله در اختیار شما دوستان قرار می گیرد . بعد از مطالعه این مقاله نظر شما و همچنین پیش فرض های شما برای تعریف و کاربردهای در های پشتی بکلی عوض خواهد شد .

جواب سوالی که از من خیلی پرسیده می شود ؟ C0llect0r به چه معناست ؟ و چرا انتخاب کردم ؟ جواب به 2 دلیل می باشد

1:اگر برق و الکترونیک خونده باشید می دونید که یکی از پایه های اصلی ترانزیستور پایه ای است بنام Collector که شدت جریان رو از پایه های دیگه به سمت خودش می کشه من هم دوست دارم که علم و هنر هک رو از تمامی منابع موجود اونهم نوع پیشرفته اش رو به سمت خودم بکشم **J** این کلمه همچنین به معنای جمع کننده علوم و اشیاء است 2: Collector همچنین نام یک سربازرس با هوش و حرفه ای در یک فیلم علمی تخیلی مربوط به آینده خیلی دور می شد که با جرایم سایبرنتیکی مقابله می کرد از جمله ربات های خلاف کار انسان نما **J** و همچنین هکر های کلاه مشکی و ....

تعاریف و انواع در های پشتی :

در گذشته ای نه چندان دور هکر ها backdoor ها را برروی سیستم ها شناسایی کرده و به آن نفوذ می کردند ولی هم اکنون دیگر بیشتر این درهای پشتی را به روی سیستمهای هدف Upload کرده ور از طریق را ه مربوطه وارد سیستم ها می شوند مزیت این گونه حملات بر این است که با استفاده از این متد دیگر هکر در هر زمانی می تواند وارد سیستم ها شود .بهتر است با تعریف اصلی یک در پشتی در ابتدا آشنا شوید بیشتر شما در های پشتی را با پورتی باز شده بر روی سیستم هدف به همراه یک سرور فایل کوچک جهت ارتباط Server/client را اشتباه می گیریداین موضوع نیز گاهی با تروجان ها نیز اشتباه گرفته می شوند اسب های تروا خود یک نوع برنامه مجزا بوده که خود متد در های پشتی یک دسترسی با توجه باامکاناتشان را فراهم می نمایند پس نباید تروجان ها را با در های پشتی نیز اشتباه گرفت بلکه باید بگویم یکی از انواع در های پشتی برای نفوذ به این شکل استفاده می شود تروجان ها علاوه بر باز کردن در های پشتی برای یک نفوذ گر امکانات و ابزار دیگری را هم فراهم می کنند شاید به علت تشابه بعضی در های پشتی با تروجان های تک منظوره جهت باز کردن یک در پشتی این خلط مبحث پیش آمده است . آن هم به خاطر کاربر آن در Web Hacking و غیره ... می باشد که به صورت کاربردی آشنا در آمده است

تعریف درهای پشتی Backdoors به صورت علمی

Backdoor

برنامه ای است که به یک نفوذ گر این امکان را می دهد تا پروسه امنیتی یک سیستم را دور زده و منابع مختلفی از آن سیستم را از راه مربوطه در اختیار نفوذ گر قرار دهد

تعداد بسیار زیادی از انواع در های پشتی قابل ذکر می باشد همانطور که طبق تعریف بالا مشاهده می کنید مبنای اصلی که به یک در پشتی مربوط می شود به دستیابی یک نفوذ گر به منابع سیستمی از طریق در پشتی تعریف می شود.این دسترسی می تواند به شکل های گوناگونی صورت گیرد که این موضوع بستگی به هدفی دارد که هکر از به کار گیری درهای پشتی دنبال می کند به طور مثال :

انواع در های پشتی Backdoors

- تغییر در سطح دسترسی محلی :

این نوع درپشتی به نفوذ گر این امکان را می دهد که ناگهان یک حساب کاربری معمولی به حساب کاربری با دسترسی به Root یا Administrator تبدیل شده و ارتقاء یابد با این دسترسی نامحدود نفوذ گر می تواند دوباره فایل های ذخیره شده بر سیستم را به طریق خود پیکر بندی نماید

- اجرای فرمانهای منفرد از راه دور

در این نوع ار درهای پشتی هکر می تواند با ارسال پیغام به سیستم هدف در همان لحظه یک تک فرمان را بروی ماشین مورد نظر اجرا کند در پشتی فرمان تکی هکر را اجرا کرده و نتیجه را به هکر باز می گرداند

- دسترسی به یک سطر فرمان از سیستم هدف از راه دور

این یکی از شناخته شده ترین در های پشتی برای هکر ها می باشد نام معروف این نوع Remote Shell است . در این نوع در پشتی به هکر این امکان را می دهد در سطر فرمان سیستم قربانی و از طریق شبکه فرمانهایی را به طور مستقیم اجرا نماید در این نوع نفوذگر می تواند سطر فرمان را به یک ابزار کاربردی تبدیل نماید از جمله توانایی انجام یک سری فرمان ها به طور موازی و یا نوشتن Script ها خطرناک و یا انتخاب دسته از فایل ها بر ای جمع آوری شان .با برسی بیشتر می توان گفت که Remote Shell ها بسیار پر توان تر و پر کاربرد تر از اجرای فرمان های تکی بر روی سیستم هدف می باشند به تشابهی این نوع در پشتی یک دسترسی مستقیم به کیبورد سیستم هدف برای شما تهیه می نماید

- دسترسی از راه دور به ماشین هدف از طریق برنامه های GUI

بعد از گذراندن مراحل دسترسی های سطر فرمان به ماشین هدف به در های پشتی می رسیم که یک دسترسی به GUI از سیستم هدف را برای ما تهیه می نمایند به طور مثال باز و بسته شدن پنجره ها یا حرکت موشواره ..در این نوع شما می توانید نظاره گر فعالیتهای قربانی بر روی سیستم اش باشید یا خود می توانید کنترل GUI سیستم مورد نطر را در دست بگیرید

با توجه به هر کدام از انواع در های پشتی ذکر شده در بالا یک نفوذ گر می تواند بر روی سیستم مورد نظر خود مانور کند از جمله فایل هایی از ماشین قربانی را در یافت کند یک سری پیکر بندی های مورد نظر خود را از دوباره اجرا نماید و غیره .توجه به این نکته لازم است که بحث ما مربوط به Defacement از طریق در های پشتی را شامل نمی شود

بلکه باید بگویم این عمل یکی از اهدافی می تواند باشد که یک نفوذ گر بعد از دستیابی به منابع یک وب سرور از طریق در پشتی اقدام به آن می کند بحث ما در این مقاله به تعریف و روش های ایجاد و و گونه های مختلف در های پشتی متمرکز می باشد نه استفاده هایی که می شود بعد از آن نمود. طیف گسترده ای از اهداف را می شود پس از ایجاد یک در پشتی دنبال کرد که کی از نوع مطلب فوق نیز می تواند باشد .پس مطلب در های پشتی را با کاربرد های ویژه این مقوله اشتباه نگیرید .بحث ما یک بحث انتزاعی و محض در مورد در های پشتی خواهد بود نه کاربردی .

روش های متداول نصب BackDoors

برای درک توانای های در های پشتی بایستی یکی از انواع در های پشتی را یر روی سیستم های هدف نصب نمایید .شاید شما شگفت زده شوید که چگونه نفوذ گران در های پشتی را بر روی سیستم ها نصب می کنند تا بتوانند در مواقع لزوم بتوانند بدون هیچ درد سری داخل سیستم های مورد نظر شوند همیشه اولین چیزی که به ذهن یک هکر بعد از نفوذ به یک سیستم خطور می کند نصب یک در پشتی مخفی برای دسترسی ها آسان تر برای دفعات بعدی می باشد مثلا یک نفوذ گر را در نظر بگیرید که از طریق Buffer Over Flow یا از طریق یکی از پیکر بندی های رایج و معمول سیستمها به سیستمی نفوذ کرده است دومین مرحله ای که به سراغ آن می رود نصب یک در پشتی می باشد نفوذ گر می تواند از طریق ویروس ها یا کر م های نیز در های پشتی ای را بر روی سیستم ها نصب نمایند .یکی دیگر از طرق نصب در های پشتی به غیر از آسیب پذیری ها گول زدن کاربران از طریق نصب یک در پشتی به دست خود کاربر است شاید هم از طریق فرستادن نامه ای به جهت نصب ویژگی های File Sharing تا کاربر آن را بروی هارد دیسک خود بنویسد شاید نام مهندسی اجتماعی برای گزینه اخیر بهتر باشد شاخه ای از این مربوط به اسب های تروا می شود که در درون خود برنامه جهت نصب یک یا چند در پشتی را شامل می شود
در مبحث بعدی برای مقابله با در های پشتی به نکتاتی اساسی اشاره می کنم .یکی از ویژگی های در های پشتی این است که به طور خودکار و اتوماتیک و بعضا در بیشتر اوقات مخفی و محرمانه بر روی سیستم ها لود شده و آماده به کار می شوند این یکی از نکاتی است که برای آسیب رساندن و بستن درهای پشتی سیستم اتان از آن استفاده خواهد کرد در مباحث بعدی با بعضی ار نمونه ها و ابزار های در های پشتی آشنا خواهید شد

روش های لود شدن در های پشتی به صورت خود کار و مخفی

بعد از نفوذ به یک سیستم و نصب یک در پشتی نفوذ گر آنرا به طور دستی فعال می نماید ولی بعد از خارج شدن از حوزه دسترسی به منابع یا همان Log Out دیگر نمی تواند به آن در پشتی برای بار دوم وصل شود به این منظور نفوذگر در پشتی را به صورتی نصب می کند و در جاهایی از سیستم قرار می دهد که با هر بار راه اندازی سیستم هدف در پشتی هم به همراه Boot Up راه اندازی شود و بدین وسیله نفوذ گر بتواند هر موقع که خواست بدون استفاده دوباره از آسیب پذیری های مورد استفاده اش در مرحله نفوذ با نصب در پشتی به سیستم قربانی وارد شود. برای این که در های پشتی سیستم ها را بشناسید و در صورت پیدا نمودن تعدادی از آنها بتوانید جلویشان را سد نمایید بایستی اول بدانید که از چه طرقی در های پشتی Run می شوند (بحث ما در

این بخش به سیستم های ویندوز محدود خواهد شد – در مورد سیستمهایی از قبیل یونیکس نیز می توانید با آدرس های فوق جهت اطلاعات بیشتر ارتباط برقرار کنید)

شناسایی در های پشتی از طریق شناسایی متد های را ه اندازی خودکار در ویندوز

سیستم های مبتنی بر ویندوز خود نیز تواناییها و روش های متفاوتی را برای راه اندازی خود کار برنامه ها به کار می گیرند که در ها پشتی نیز با استفاده از یکی یا چند تا از روش های زیر به راه اندازی اتوماتیک خود دست می زنند .

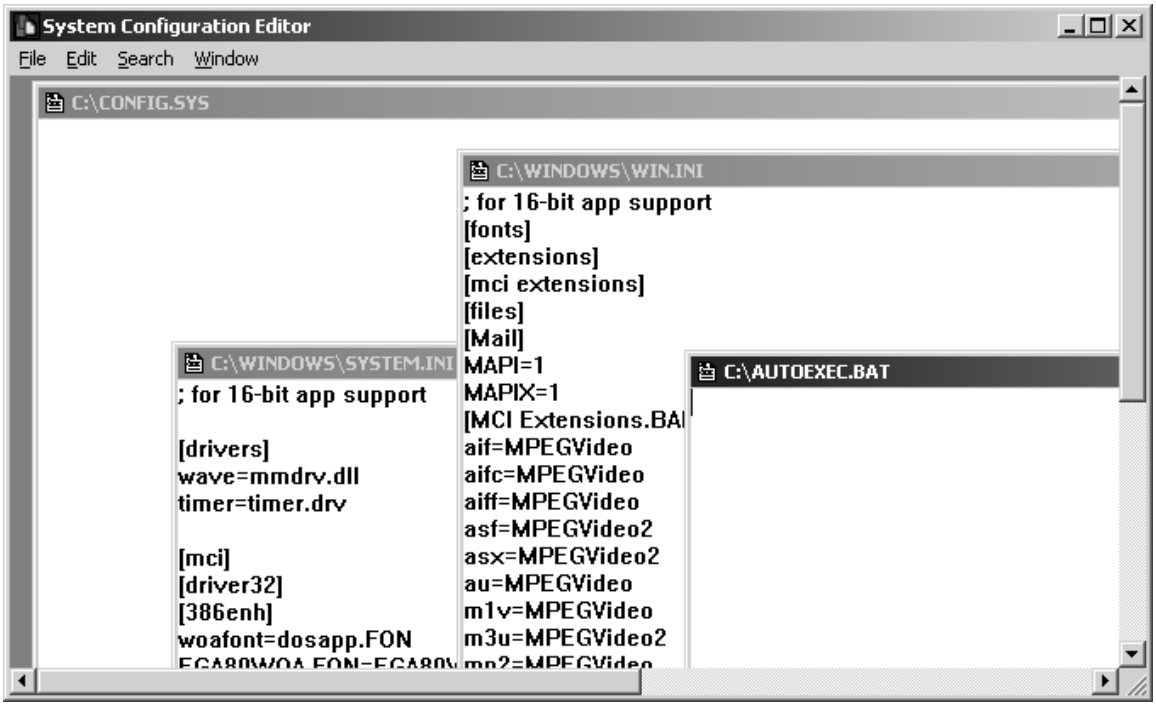
فایل ها و پوشه های Startup در ویندوز
در این مرحله می خواهیم مقداری در مورد فایل ها و پوشه هایی از ویندوز با شما صحبت کنیم که در شرایطی از قبیل بوت شدن سیستم فایل های اجرایی یا اسکریپت ها و یا پروسه هایی را یه صورت خود کار اجرا می کنند نفوذ گر می توانند بر روی هدف مورد نظر برنامه در پشتی خود را در یکی از این فایل ها و یا پوشه ها قرار داده یا مسیر دهی کند به راهنمای زیر توجه کنید

Windows Startup Files and Folders	
File or Folder Name	**How File or Folder Can Be Altered to Automatically Activate a Backdoor**
Autostart Folders	The attacker places the backdoor or a link to it in these folders, which are activated at startup or while a user logs on to the system. On Win95/98/Me, a single folder holds this information, located at C:\Windows\Start Menu\Programs\StartUp. WinNT/2000/XP/2003 systems include an autostart folder, usually associated with "All Users," as well as individual autostart folders for individual users, located at the following locations: • WinNT— C:\Winnt\Profiles\[user_name]\Start Menu\Programs\StartUp • Win2000— C:\Documents and Settings\[user_name]\Start Menu\Programs\StartUp and (if upgraded from Windows NT) and C:\Winnt\Profiles\[user_name]\Start Menu\Programs\StartUp • WinXP/2003— C:\Documents and Settings\[user_name]\Start Menu\Programs\Startup
Win.ini	Win.ini contains information about initializing the operating system. This file can be altered to start a backdoor in two ways. First, it could directly execute a program referred to in the file, using the text "run=[backdoor]" or "load=[backdoor]". Second, it could associate some suffix (e.g., ".doc" or ".htm") with a backdoor program that would run every time a file with such a suffix is executed by the system. This file location varies, but is

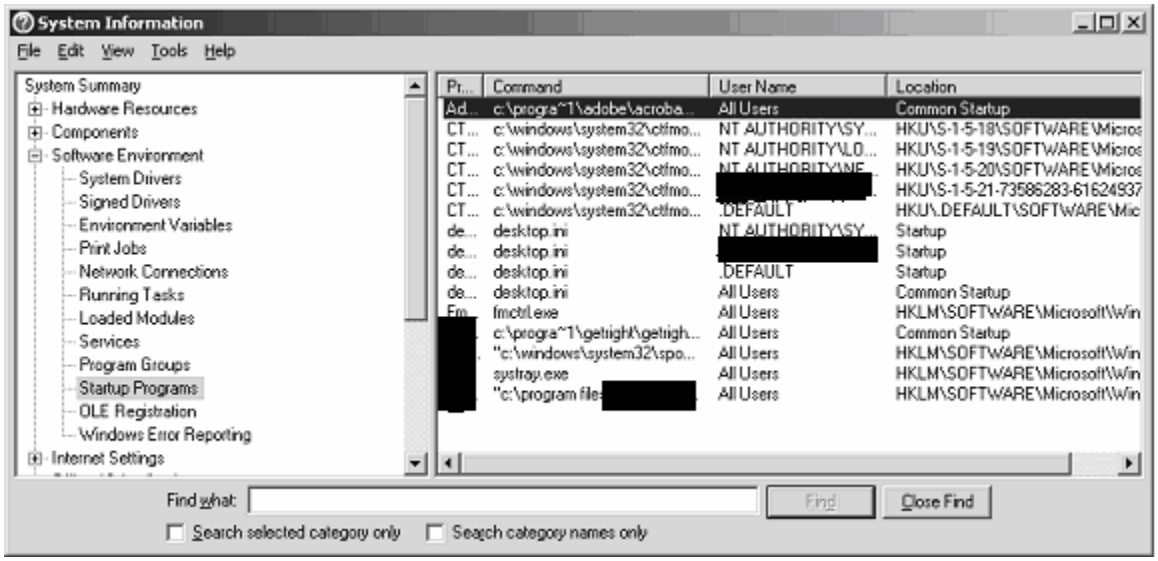
Windows Startup Files and Folders	
File or Folder Name	**How File or Folder Can Be Altered to Automatically Activate a Backdoor**
	typically located in: • Win95/98/Me— C:\Windows\win.ini • WinNT/2000— C:\Winnt\win.ini • WinXP/2003— C:\Windows\win.ini
System.ini	This file contains settings for the system's hardware. On Windows 3.X and Windows 9X, this file supported the "shell=" command, which is used to specify a user shell to launch at system boot time. The shell will be the main interface program that all users see when they boot the machine. Attackers often modify the line "shell=explorer.exe" so that, instead of starting up the Windows Explorer GUI, the system executes a backdoor while the system boots. The backdoor then, in turn, starts the actual user's shell, which is usually explorer.exe. On more recent Windows versions (WinNT/2000/XP/2003), the operating system ignores the "shell=" syntax in System.ini. Therefore, this method isn't used to start a backdoor on these newer operating systems. This file is usually located in the following places: • Win95/98/Me— C:\Windows\System.ini • WinNT/2000— C:\Winnt\System.ini • Windows XP/2003— C:\Windows\System.ini
Wininit.ini	This file is created by Setup programs when new software is installed and some action is required by the system to complete the installation after reboot. For example, when you install a new hardware driver, your install program might make you reboot the system. As the system is rebooting, an entry in Wininit.ini will run some program during the boot process. Alternatively, this file can be used to steal the name of some commonly used executable and assign it to a backdoor. When it is used, the file is usually located in: • Win95/98/Me— C:\Windows\wininit.ini • WinNT/2000— C:\Winnt\wininit.ini • Windows XP/2003— C:\Windows\Wininit.ini
Winstart.bat	In older Windows systems (Win 9X), this file is normally used to start old MS-DOS programs in a Windows environment. An attacker could include a line with the syntax "@[backdoor]" to run an executable and hide it from the user. If it is present, it will typically be located in

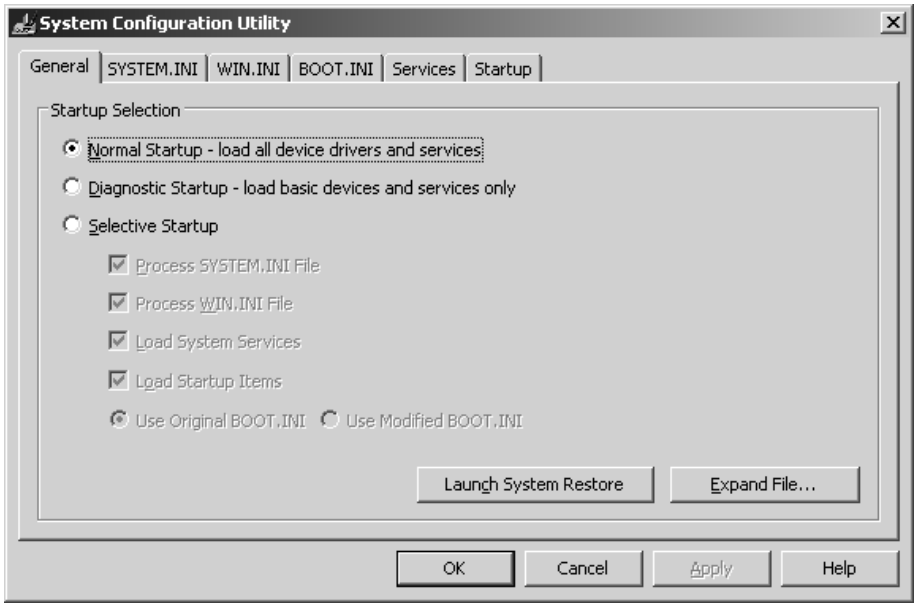
Windows Startup Files and Folders	
File or Folder Name	**How File or Folder Can Be Altered to Automatically Activate a Backdoor**
	C:\Winstart.bat.
Autoexec.bat	This file is relevant only on Windows 95/98 systems. It is ignored on Windows Me, NT, 2000, XP, and 2003. For backward compatibility, it supports launching programs by simply including a line that refers to the program file, such as "C:\[backdoor]". If it is present, it will typically be located in C:\Autoexec.bat.
Config.sys	This file is relevant only on Windows 95/98 systems. It is ignored on Windows Me, NT, 2000, XP, and 2003. This file loads low-level MS-DOS-based drivers, and is not included on some Windows systems. It could include a line to execute a backdoor. If it is present, this file is usually located in C:\Config.sys.

برای دسترسی به فایل ها ی مورد نظر به سطر فرمان یا Run رفته و با اجرای فرمان Sysedit برنامه System Configuration Editor را باز نمایید در برنامه مورد نظر system.ini-win.ini-config.sys-autoexec.bat قابل دسترس می باشند برای فایل های دیگر نیز به شاخه ها و پوشه های اشاره شده مراجعه کنید



نقاط دیگری که خواهید توانست به فایل ها و فولدر های اجرایی دسترسی پیدا نمایید می توان به System Information و همچنین System Configuartion Utility خود ویندوز اشاره نمود (به تصاویر زیر توجه کنید)





البته برنامه های ذکر شده جزو برنامه ها و ابزار های داخلی ویندوز می باشند که برای همگان آشنا هستند در ادامه به چند برنامه دیگر نیز برای یافتن نشانه هایی از در های پشتی اشاره خواهم کرد البته به هر کدام از فایل ها و پوشه های مورد نظر نیز می توانید با توجه به مسیر داده هر کدامشان مراجعه نمایید

استفاده از رجیستری Registry

بعد از فایل ها و فولدر ها نوبت به کلیه کلید های مدخل رجیستری ویندوز می رسد قبل از شروع به این بحث باید به یک تذکر جدی اشاره کنم که قبل از هرگونه دست کاری نا آگاهانه رجیستری ویندوز از آن یک نسخه پشتیبان جهت مواقع اظطراری تهیه کنید و یا اگر تجربه کافی در این زمینه را دارید به اعمال تغییرات بر روی رجیستری ویندوز اقدام کنید رجیستری ویندوز یکی از نقاط حساس و آسیب پذیر این سیستم عامل می باشد از جهاتی بسیار شبیه عملکرد ژنوم انسانی است که ممکن است کوچکترین اشکال در یک مدخل به بزرگترین آسیب ها تیدیل شود قبل از ادیت رجیستری به کتاب های آموزشی و راهنمای موجود در این زمینه مراجعه نمایید خود من استفاده از کتاب الکترونیکی زیر را پیشنهاد می کنم

خوب به مدخل های رجیستری در زیر توجه کنید برای ادیت هر کدام از این مدخل ها با توجه با آدرس مورد نظر توسط برنامه Registry Editor داخل ویندوز مراجعه نمایید

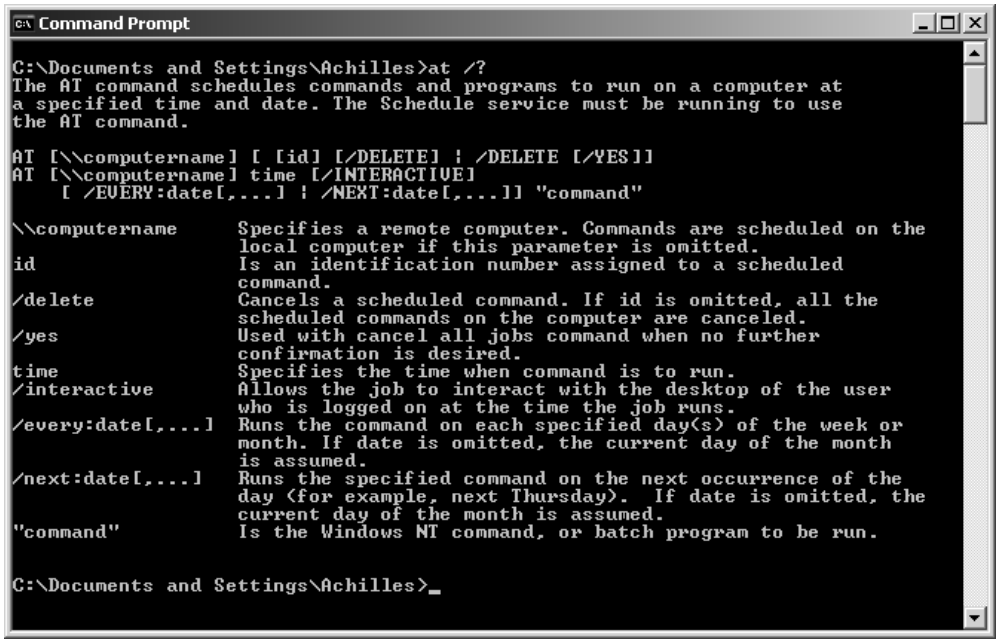
Registry Keys That Start Programs on Login or Reboot	
Registry Key	**Purpose of the Key**
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\RunServicesOnce	Some programs are installed to run in the background on a Windows machine as a service, such as the IIS Web server or file and print sharing services. This registry key identifies which services should be started during the next reboot and the next reboot only. For all subsequent boots, the services will not be started.[1]
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\RunServices	This registry key contains a list of services to be launched at every system boot.
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\RunOnce	This registry key identifies which programs (not services) should be started during the next reboot and the next reboot only. For all subsequent boots, the programs will not be executed.
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Run	These programs are executed during system boot.
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\RunOnceEx	Only available on Windows 98 and Me, this registry key indicates scripts and programs that are to be run at boot time, but shouldn't be started as separate processes. To improve efficiency, these programs are not run as separate processes, but are instead invoked as separate threads within various other boot processes.[2]
HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon\Userinit	This key contains the names of programs to be executed when any user logs onto the system. It typically indicates the user's GUI.[3]
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\ShellServiceObjectDelayLoad	This registry key activates programs after the Windows GUI starts up, such as the system tray in the bottom

Registry Keys That Start Programs on Login or Reboot	
Registry Key	**Purpose of the Key**
	right-hand corner of Windows and its contents.
HKLM\SOFTWARE\Policies\Microsoft \Windows\System\Scripts	This key identifies various scripts that will be executed when Windows boots up.
HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\Explorer\Run	The programs identified by this registry key are started when the user GUI (explorer.exe) is activated.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\RunServicesOnce	This registry key identifies which services should be started the next time a user logs on, one time only. For all subsequent logons, the programs will not be executed.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\RunServices	These services are started every time a user logs onto the system.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\RunOnce	These programs are activated once when a user logs onto the system.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\Run	These programs are run every time a user logs onto the machine.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\RunOnceEx	These programs are executed without starting another system process.
HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\Explorer\Run	These programs are run each time a user logs onto the system.
HKCU\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Windows\Run	These programs are run each time a user logs onto the system.
HKCU\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Windows\Load	These programs are run each time a user logs onto the system.
HKCU\SOFTWARE\Policies\Microsoft \Windows\System\Scripts	These scripts are activated every time a user logs onto the machine.
HKCR\Exefiles\Shell\Open\Command	This key indicates programs that will be run any time another EXE file is executed, a very frequent occurrence on a Windows machine, to be sure!

روش آخر و عمومی استفاده از Task Scheduled ویندوز می باشد در این روش در پشتی از Scheduled ویندوز های NT/2000/XP/2003 استفاده می کند با استفاده از سرویس

هکر می تواند به سیستم بگوید که چه نوع برنامه خاصی و در چه Task Scheduled وقتی راه اندازی شود حتی می توان تاریخ مورد نظر و یا با تعیین بوقوع پیوستن اثری در رایانه بار شدن برنامه در پشتی را تنظیم نمود مثل هنگام بوت شدن یا logon کردن با ویزارد برنامه Scheduled Task می توانید به راحتی این تنظیمات را اعمال کنید

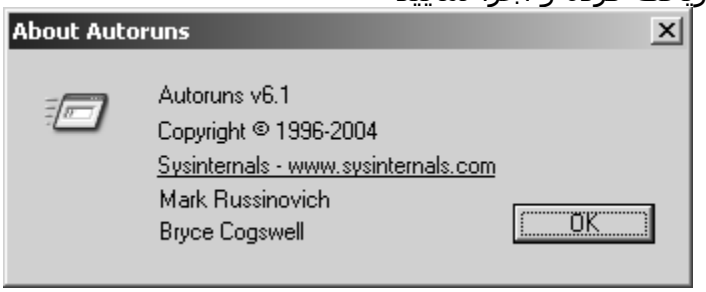
بعد از انتخاب برنامه های مورد نظر می توانید با استفاده از برگه properties در پنجره Scheduled Task زمان و دیگر پارامتر ها را تعیین کنید .با استفاده از سطر فرمان نیز و با استفاده از فرمان at کار مشابهی نظیر GUI فوق را انجام دهید



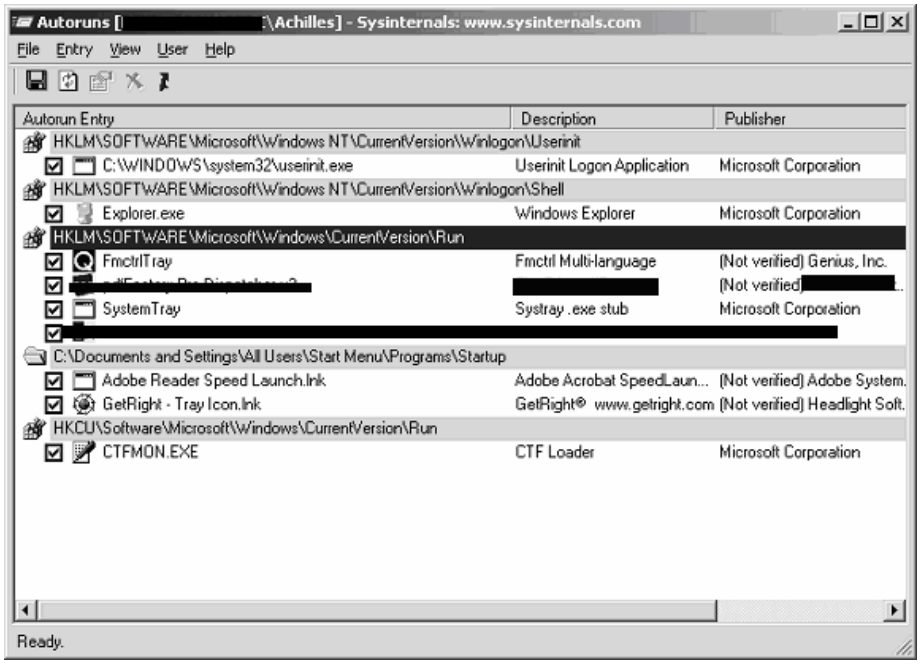
تا اینجا شما با تعاریف و نحوه های را اندازی برنامه ها از طرق مختلف به طور مفصل آشنا شدید در اینجا می توانم به این نکته اشاره کنم که شما هم اکنون به تمامی فرمان ها و روش ها و همچنین متد های بار کردن خودکار برنامه ها و فایل ها آشنایی کاملی را پیدا کردید تا این جا شما با فرمان ها و همچنین ابزار های داخلی ویندوز آشنا شدید اما این آشنایی کافی نیست اطلاعاتی که اغلب از این ابزار ها بدست می آورید کامل نیستند و بسیاری از جزیات بخصوص در باره ی اسکریپت ها را در اختیار شما قرارنمی دهند باید یک هکر بسیار واضح و آشکار یا به قولی خیلی باید یک Backdoor رو روی سیستم ما خیلی محسوس نصب کنه تا ما با این ابزار داخلی تشخیص بدهیم در ظمن رجوع تک تک به هر کدوم از این مدخل ها کار خسته کننده ای می تونه باشه .خوب همیشه برای را ه های تکراری و این شکلی متخصصان هستند که کار استفاده کنندگان رو راحت می کنند در اینجا من یک برنامه مجانی و جالب رو به شما معرفی می کنم که در آن واحد نه تنها تمامی مدخل های گفته شده رو البته تقریبا همه آنها رو در اختیار شما قرار می دهد بلکه امکانات متعد دیگری رو هم از جمله اطلاعات اضافی در برنامه هر برنامه در حال اجرا رو نشان می دهد

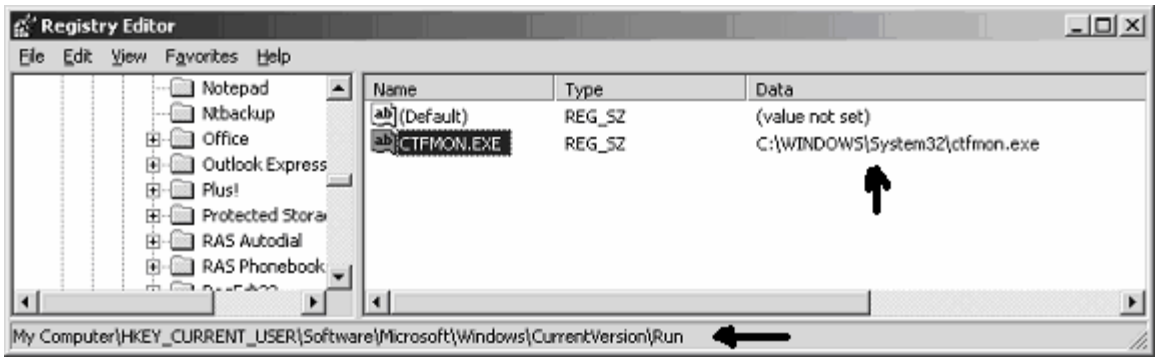
برنامه : Autoruns این برنامه را که به صورت Free می باشد را می توانید با مراجعه به آدرس www.sysinternals.com/ntw2k/source/misc.shtml#autoruns, به همراه ده ها ابزار دیگر که همگی آنها ابزار های تکمیل کننده ابزار های داخلی مربوط به ویندوز هستند را دریافت کنید استفاده از برنامه های دیگر این سایت را پیشنهاد می کنم البته نه همه آنها مثل همین AutoRunو از جمله Process Exploree که تکمیل کننده Task Manager می باشد از جمله برنامه های سایت هستند

برنامه Autoruns به همراه نسخه سطر فرمان آن به نام Autorunsc در حدود 150 KB حجم دارد آن را دریافت کرده و اجرا نمایید



بر روی هریک از گزینه ها دابل کلیک نمایید شما را مستقیما یا به مدخل رجیستری و یا فابل یا پوشه مورد نظر خواهد برد برای مثال من بر روی CTFMON.EXE دابل کلیک می کنم





از ویژگی های برنامه Autoruns این است که تمامی برنامه های پنهانکار و Stealth Mode را شناسایی و نمایش می دهد اما یک Bug ای که خود من به آن در این برنامه پی بردم این است که این برنامه یک اسکنر Time Basedاست به این معنی که تمامی فایل ها و پروسه هایی را شناسایی می کند که از روش فعالسازی خودکار سیستم بار شده اند توضیح بیشتر اینکه اگر نفوذ گر برنامه ای را توسط برنامه Scheduled Tasks برای ساعت 3 بامداد تنظیم کند و شما مثلا در نیمه روز با AutoRuns سیستم را اسکن نمایید هیچ در پشتی را بر روی سیستم شناسایی نخواهید کرد برای حل این Bug نرم افزار می توانید با مراجعه دستی یا manual به منابع و مدخل های اشاره شده بهره بگیرید
یک تمرین ساده به دوستتان بگویید که در غیاب شما بر روی سیستم اتان یک Backdoor ایجاد کند و بعد ببینید شما قادر خواهید بود که در پشتی مورد نظر را با توجه به آموخته هایتان کشف کنید
همانطور که می دانید ابزار هایی نیز به جهت جستجوی خودکار ابزار های جاسوسی طراحی شدهاند البته یک قسمت از این برنامه ها مخصوص چک کردن مدخل ها از نظر در های پشتی می باشد از قبیل :

خودتان نیز می توانید با رجوع با قسمت های گفته شده از وجود یا عدم وجود در های پشتی اطمینان پیدا کنید که البته برای این موضوع نیاز به مقداری تجربه دارید

ویروس یا کرم یا در پشتی یا اسب تروا

خوب در کل ما در این مقاله در باره ی نوع و محل های راه اندازی در های پشتی با شما صحبت کردیم برای اینکه تشخیص بدهید که آیا یک فایل که در رجیستری قرار دارد مربوط به یک برنامه مجاز داخل سیستم خودتان است یا مربوط به یک برنامه کاربردی است که خودتان نصب نموده اید یا در حالت خطرناکتر مربوط به یک کرم یا یک ویروس و یا همین بحث خودمان یک Backdoor است باید چه کار کنید اغلب بحث بر روی ویروس ها و کرم ها و همچنین Backdoor ها به خاطر تشابه مسایل با هم اشتباه گرفته می شوند باید در کل بگویم که یک ورم یا ویروس از لحاظ عملکرد و یا ساختار در بسیاری از جهات شبیه به هم هستند ولی از نظرتعریف بسیار متفاوت می باشند مثلا خیلی افراد اظهار می کنند که ویروس ملیسا یا ویروس ساسر که این کاملا اشتباه است بلکه باید به این ها کرم اطلاق شوند یک مثال مناسب برای ویروس ها برنامه مخرب و یا همان ویروس چرنوبیل بودطبق تعریف کلاسیک ویروس ها برنامه های مخربی هستند که از سورس کدهای مخرب ایجاد شده به منظور ضربه زدن به سخت افزار و نرم افزار موجود در رایانه ها در کلام بعدی به ساده ترین صورت ویروس قابل انتقال در شبکه را که قادر به کپی برداری از خود بوده و در نسخه های پیشرفته تر هوشمند بوده و پنهانکار هم هست را ورم گویند می تواند هم مخرب باشد و هم بی ازار می تواند در داخل خود نر م افزار های جاسوسی را به همرا ه داشته باشد یا نه به هر حال به شکل عامیانه ویروس متحرک در شبکه را کرم های رایانه ای می گویند که با استفاده از پروتکل هایی از جمله POP3 و یا FTP در شبکه منتشر می شوند -اسب تروا نه ورم است و نه ویروس بلکه یک فایل به ظاهر بدون خطر می باشد ولی در دل خود برنامه ای مخرب به همراه دارد حالا این برنامه می تواند در پروسه کاری اش بعد از اجرا شدن در سیستم قربانی به تک تک دستور العمل های داده شده بپردازد مثل نظاره گری و ثبت ضربه زنی های کیبورد و ارسال آنها و ده ها مورد دیگر
خوب تکلیف در پشتی در اینجا چیست در پشتی با این که یک برنامه است ولی هیچ کدام از سه نوع بالا نمی باشد طبق مطالب بالا در پشتی یک نوع **دسترسی** برای نفوذگر می باشد که حال این متد دسترسی می تواند به شکل های گوناگون در سه شکل بالا به کار گرفته شود –در کل منظور من از آوردن این بحث این است که خود در های پشتی نمی توانند به خودی خود آسیبی به سیستم شما وارد کنند تا زمانی که آز آن برای ورود ناگهانی و مخفی استفاده نشود اما این به آن منزله نیست که خطر در های پشتی را کمتر از خطر ویروس ها و کرم هها و ترو جان ها در نظر بگیرید بلکه منظور من این است که تا وقتی که به شبکه متصل نباشد از شر یک نفوذ گر در امان خواهید ماند ولی آیا برای یک سرور هم به همین منوال است ؟خیر - حتی به نظر من خطرناک تر از ویروس و کرم برای سرور های متصل به شبکه یک در پشتی و مخفی می باشد به این ترتیب اولین گام خطرناک یک نفوذ به شمار می رود – در کلام آخر این بخش باید بگویم که برای شناسایی برنامه های معروف backdoor نصب شده یر روس سیستم هایتان بایستی حداقل با یک یا چند تا از معروفترین آنها آشنا شوید برای این منظور به بخش بعدی توجه فرمایید بعد از آشنایی با بخش مذبور و شناسایی هر یک از برنامه های گفته شده و با توجه با اطمینان از در پشتی بودنشان به از بین بردن و مسدود کردن آنها اقدام کنید

SECRET AREA

توجه

از انجا که مقاله حال حاظر پیش روی شما یک مقاله White Paper می باشد و قصد آن آموزش هکینگ و نصب انواع backdoors بر روی سیستم ها و سرور ها نمی باشد به بحث بر روی انواع و چگونگی عملکرد دقیق این برنامه ها به طور مفصل نخواهیم پرداخت فقط از جهت آشنایی علاقه مندان به این مباحث و همچنین شناسایی انواع برنامه های به کار رفته شده در جهت تولید و نصب در های پشتی اشاراتی می شود امید است دوستان علاقه مند با توجه به راهنمایی های مذبور خود به دنبال کسب اطلاعات بیشتری در این زمینه ها باشند

ملاحظات :
لازم به تذکر است کلیه مطالب گفته شده در این بخش از مقاله صرفا جنبه آموزشی دارد.و هر گونه استفاده غیر آموزشی از این مطالب بر عهده خود کاربران میباشد .و نویسندگان این مقاله ومدیریت سایت امنیت وب هیچ گونه مسوولیتی را در قبال ان ندارند

NetCat

فکر می کنم این ابزار آنقدر دیگر معروف باشد و آنقدر با آن آشنا باشید که چگونگی نحوه کار و همچنین دستور ها و سوئیچ ای آنرا به کلی فرا داشته باشید ولی یک نکته ای که الان به ذهن من می رسد این است که نفوذ گران بعد از عملیات نفوذ برای جلوگیری از شناسایی فایل Netcat.exe ان را با نام دیگری تغییر نام می دهند و اغلب هم برای گم راهی کاربران خبره تر و همچنین ابزار های یابنده این در های پشتی با اضافه کردن اعداد یا حروفی آنرا مخفی تر می نمایند مثلا به جای استفاده از nc از SVHOST که تشابه زیادی با یکی از زیر پروسه های اجرایی ویندوز به نام SVCHOST استفاده می کنند که به یاد داشتن این نکته خالی از لطف نیست .برای ایجاد یک در پشتی می توان از برنامه نت کت طوری استفاده نمود که پورتی بر روی سیستم هدف را باز کرده و پشت آن پورت یک برنامه را به حالت Stand By نگاه دارد که اغلب بر روی سیستم های ویندوز کنسول سطر فرمان یا همان Cmd خودمان است بر روی سیستم های یونیکس نیز یک جلسه کاری یا Session را فراخوانی میکند بعد از این مرحله هکر می تواند بسیار راحت توسط تل نت یا همان نت کت از برنامه ای که پشت پورت باز شده قرار دارد ارتباط برقرار نماید

Using Netcat 4 Backdoors Purpose

```
In Wind0Z
nc [options] target_system_name [remote_port]

C:\>  nc –l –p [port_number] –e cmd.exe
C:\>  nc –vvv [victim_address] [port_number]
In *NIX
$ nc –l –p [port_number] –e /bin/sh
$ nc [victim_address] [port_number]
```

در بالا چگونگی یکی از کاربرد های انگشت شمار نت کت را ملاحظه نمودید ولی یکی از اشکال هایی که هکر ها کمتر به آن توجه می کنند اینست برنامه نت کت فرمان ها و اطلاعات را به صورت Clear Type ارسال و در یافت می کند که یک مدیر شبکه با هوش و یا یک سیستم شناسایی دخول IDS و یا حتی یک هکر دیگر با Sniff می تواند ارتباطات را شناسایی کرده و آن ها را باز آوری کند برای همین ابزاری برای Encryption نت کت و ارتباطات آن ایجاد شده است به نام Cryptcat که می توان همان امکانات نت کت را در اختیار داشت به اضافه یک ارتباط رمز شده.
برنامه های مشابه همانند نت کت با این خصوصیات در شبکه بسیار یافت می شود از قبیل:

برنامه های دیگر همانند نت کت

- Tini
- Q
- BindShell
- MD5BD
- UDP_Shell
- TCP_Shell

حفاظت در برابر برنامه های Shell گیری

همانطور که تا کنون پی بردید بحث ما بر روی یک در پشتی متمرکز می باشد به تشابهی اگر کامپیوتر را به خانه ای مثال بزنم در یک خانه معمولی که محل ورود و خروج افراد می باشد پورت های یک سیستم نیز به نوعی در های ورود و خروجی اطلاعات و پکت ها برای رایانه می باشند حال اینها اطلاعات مفید باشند و یا اطلاعات مخرب باشند یکی از راه های ورودی پورت های سیستم ها می باشند پس دیگر بحث اضافی لازم نیست اولین خط مقدم در برابر حملات Shell گیری حفاظت از پورت های سیستم هایتان می باشد .بحث ما بیشتر بر روی پورت های مجازی معطوف است تا پورت های فیزیکی و سخت افزاری طبق استانداردها پورت های مجازی دارای سقفی د رحدود 65535 پورت را شامل می شود که خود این دامنه به سه دسته جهت کاربری راحت تر تقسیم می شود

1

: پورت های 1-1023

شاید بتوان گفت بیشتر کاربا این پورت ها صورت می گیرد به این دسته پورت های شناخته شده و معروف نام می برند بسیاری از پروتکل های معروف نیز در این حوزه از پورت ها فعالیت می کنند به جدول زیر توجه فرمایید - به تعدادی از پورت های معروف این گروه توجه فرمایید

Well Known Ports

Service	Port	Comments
TCP Ports		
echo	7/tcp	
discard	9/tcp	sink null
systat	11/tcp	users
daytime	13/tcp	
netstat	15/tcp	
qotd	17/tcp	quote
chargen	19/tcp	ttytst source
ftp-data	20/tcp	
ftp	21/tcp	
telnet	23/tcp	
smtp	25/tcp	mail
time	37/tcp	timserver
name	42/tcp	nameserver
whois	43/tcp	nicname
nameserver	53/tcp	domain
apts	57/tcp	any private terminal service
apfs	59/tcp	any private file service
rje	77/tcp	netrjs
finger	79/tcp	
http	80/tcp	
link	87/tcp	ttylink
supdup	95/tcp	
newacct	100/tcp	[unauthorized use]
hostnames	101/tcp	hostname
iso-tsap	102/tcp	tsap
x400	103/tcp	
x400-snd	104/tcp	
csnet-ns	105/tcp	CSNET Name Service
pop-2	109/tcp	Post Office Protocol version 2
pop-3	110/tcp	Post Office Protocol version 3
sunrpc	111/tcp	
auth	113/tcp	authentication
sftp	115/tcp	
uucp-path	117/tcp	
nntp	119/tcp	usenet readnews untp
ntp	123/tcp	network time protocol
statsrv	133/tcp	

```
profile         136/tcp
NeWS                    144/tcp         news
print-srv               170/tcp
https           443/tcp         Secure HTTP
exec            512/tcp         remote process execution;
                                authentication performed using
                                passwords and UNIX loppgin names
login           513/tcp         remote login a la telnet;
                                automatic authentication performed
                                based on priviledged port numbers
                                and distributed data bases which
                                identify "authentication domains"
cmd                     514/tcp         like exec, but automatic
                                authentication is performed as for
                                login server
printer         515/tcp         spooler
efs             520/tcp         extended file name server
tempo                   526/tcp         newdate
courier                 530/tcp         rpc
conference              531/tcp         chat
netnews                 532/tcp         readnews
uucp                    540/tcp         uucpd
klogin          543/tcp
kshell          544/tcp         krcmd
dsf             555/tcp
remotefs                556/tcp         rfs server
chshell                 562/tcp         chcmd
meter                   570/tcp         demon
pcserver                600/tcp         Sun IPC server
nqs             607/tcp         nqs
mdqs                    666/tcp
rfile           750/tcp
pump                    751/tcp
qrh             752/tcp
rrh             753/tcp
tell            754/tcp         send
nlogin          758/tcp
con             759/tcp
ns              760/tcp
rxe             761/tcp
quotad                  762/tcp
cycleserv               763/tcp
omserv                  764/tcp
webster                 765/tcp
phonebook               767/tcp         phone
vid             769/tcp
rtip            771/tcp
cycleserv2              772/tcp
submit                  773/tcp
rpasswd                 774/tcp
entomb                  775/tcp
wpages                  776/tcp
wpgs                    780/tcp
mdbs            800/tcp
device                  801/tcp
maitrd                  997/tcp
busboy                  998/tcp
garcon                  999/tcp
```

2: دسته پورت های ثبت شده 1024-49151

3:دسته پورت های دینامیک یا خصوصی 49152-65535

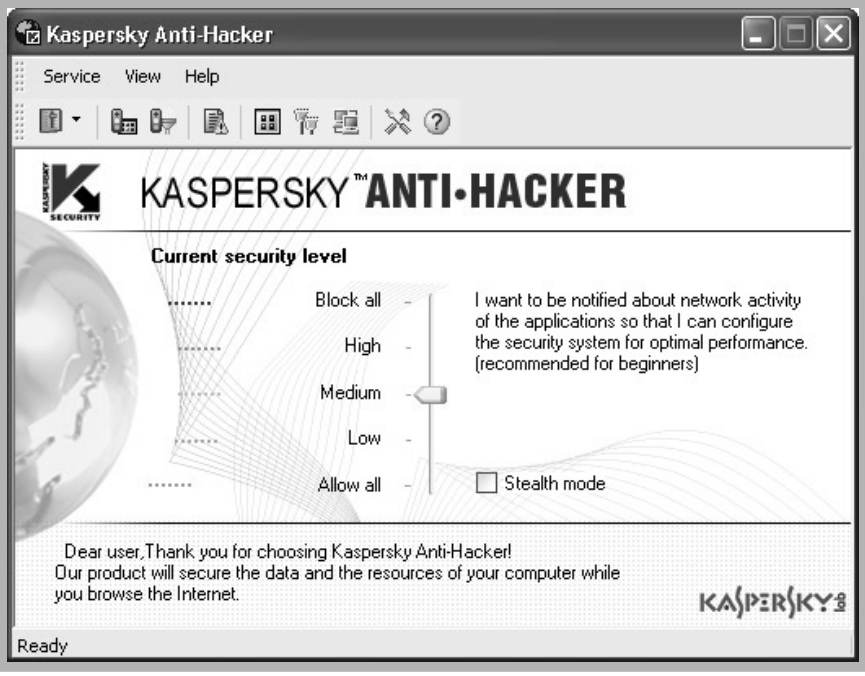
از بین سه دسته فوق بایستی دسته دوم پورت ها بیشتر باید مورد توجه اتان باشد البته Shell هایی هستند که از دیگر پورت های دسته های اول و دوم نیز استفاده می کنند ولی دسته دوم بیشتر از دیگردسته ها استفاده می شوند

یکی از بهترین توصیه ها حفاضت با دیواره های آتش Firewalls و IDS و همچنین Port Blocker ها می باشد در این زمینه نیز تعداد مقالات و همچنین نرم افزار ها بی شمار است ولی از جهت معرفی من این فایروال ها را پیشنهاد می کنم در زیر دو ابزاری را که خودم شخصا استفاده میکنم را به شما معرفی می کنم

. Personal Firewalls for Windows Systems		
Personal Firewall	**Web Site**	**Claim to Fame**
Zone Alarm	www.zonelabs.com	This tool controls both incoming and outgoing traffic by assigning specific applications to certain ports. It's available on a commercial basis, or free for noncommercial, nonprofit use (excluding educational and government organizations … the vendor employees have to feed their families somehow, I suppose).

. Personal Firewalls for Windows Systems		
Personal Firewall	**Web Site**	**Claim to Fame**
Kaspersky Anti-Hacker	www.kaspersky.com	Kaspersky Anti-Hacker is a personal firewall that is designed to safeguard a computer running a Windows operating system. It protects the computer against unauthorized access to its data and external hacker attacks from the Internet or an adjacent local network. Kaspersky Anti-Hacker: • Monitors the TCP/IP network activity of all applications running on your machine. If it detects any suspicious actions, the program notifies you and if re-quired, blocks the suspect application from accessing the network. This allows you to preserve confidential data on your machine. For example, if a Trojan tries to transmit any data from your computer, Kaspersky Anti-Hacker will block this malware from accessing the Internet. • The SmartStealth™ technique makes it difficult to detect your computer from outside. As a result, hackers will lose the target and all their attempts to access your computer will be doomed to fail. Besides, this allows for prevention of the DoS (Denial of Service) attack of all types. At the same time you will not feel any negative influence of this mode while working on the Web: the program provides conventional transparency and accessibility of the data. • Blocks the most common hacker network attacks by permanently filtering the incoming and outgoing traffic, and also notifies the user about any such attacks. • Monitors for attempts to scan your ports (these attempts are usually followed by attacks), and prohibits any further communication with the attacking machine. • Allows you to review the list of all established connections, open ports, and active network applications, and if required,

. Personal Firewalls for Windows Systems		
Personal Firewall	**Web Site**	**Claim to Fame**
		lets you terminate unwanted connections. • Allows you to secure your machine from hacker attacks without special configuration of program settings. The program allows simplified management by choosing one of five security levels: Block all, High, Medium, Low, Allow all. By default the program starts with the Medium level, which is a training mode that will automatically configure your security system depending on your responses to various events. • Allows flexibility of security system configuration. In particular, you can set the program to filter network operations into wanted and unwanted, and you can configure the Intrusion Detection System. • Allows you to log certain security-related network events to various special-purpose logs. If required, you can define the detail level of the log en-tries.



ابزار Kaspersky رو بیشتر برای حرفه ای تر ها پیشنهاد می کنم تنظیماتش یک مقدار با Zone Alarm فرق می کنه ولی از نظر من در بعضی جهات نه تنها با اون برابری می کنه شاید هم بهتر باشه ولی یک اشکالی که داره اگه خوب تنظیم نشه می تونه خیلی زود حوصله شما رو سر ببره و آخرش این میشه که از خیرش بگذرید ولی امتحانش برای یک بار ضرری نداره لازم به ذکر می باشد که گروه kaspersky که شرکتی در روسیه می باشد به تازگی بخشی از تحقیقات ضد ویروس و ضد خرابکاری رایانه ای میکروسافت را به عهده گرفته اند حتما دلیلی داشته که میکروسافت کمپانی های بزرگی مثل سیمانتک و دیگران رو ول کرده و با این گروه که در اصل همه هکر هستند رابطه بر قرار کرده در آینده بیشتر مادربورد های تولیدی مجهز به آنتی ویروس kaspersky خواهند شد

یک سوال اساسی ؟!؟!؟!
با نظر گرفتن این موضوع که اگر به خوبی از پورت های سیستم خود حفاظت کنید آیا از نظر خطر حملات شل گیری و احتمالا نصب در پشتی در آمان خواهید ماند یا نه ؟

باید بگویم جواب این سوال مطلق نیست و نسبی هم است و بستگی به هکری دارد که قصد نفوذ به شبکه شما را دارد –خوب شاید بپرسید من از همه فایر وال ها و هر نوع Removal استفاده می کنم و همیشه patch های ارائه شده رو نصب می کنم و همچنین دیگر اصول امنیتی رو هم رعایت می کنم مثل استفاده از IDS و همچنین حفاظت پورت ها و غیره ..آیا هنوز امکان ضربه خوردن ما وجود داره ؟؟؟ بله –این موضوع همانطور که یه شما گفتم بستگی به سطح هکری است که در حال نفوذ به شبکه شما است پیدا می کند اگر بیشتر اصول امنیتی که در بالا به چند تااز آنها اشاره کردم به درستی و بدون نقص اقدام کنید باید بگویم که دست بسیاری در حدود 80-90 در صد هکر ها را به منابع خودتان کوتاه کرده اید ؟ همیشه خطر از ناحیه هکر های خبره بر می خیزد آنها سدی در برابرشون وجود نداره براحتی ار خود پروتکل ها برای هک پروتکل ها استفاده می کنند استفاده از آسیب پذیری هایی که هرگز به مجامع عمومی وارد نمی شوند هم دسته دیگر هست که شما می تونید ضربه بخورید
و آن چیزی که مربوط به مقاله ما میشود در های پشتی است باید بگویم که دسته ای از در های پشتی نیز هستند که اصلا نیازی به پورت ندارند پس می بینید که دست هکر ها هم آنچنان بسته نیست اما نه هر هکری ؟شاید کم و بیش به مقداری از مطالب بالا احاطه داشتید و یاهم نه ؟ولی با اطمینان می توانم بگویم که این متد نیز یکی از معدود متد هایی هست که هم اکنون در جوامع کلاه مشکی در جریان است از این مطلب به Backdoors without Ports یاد می شود
اگر برگردیم به همان مثال قبلی شاید موضوع یک مقدار روشن تر می شود شاید بهترین راه برای نفوذ به هر خانه ای در اصلی آن و یا در پشتی آن باشد ولی آیا این ها تنها راه های ورود اهستند ؟خیر - می توان نقب زد یا از کانال فاضلاب و یا از شومینه شاید هم از تهویه مطبوع و..... این ها در محدوده درب ها و یا همان پورت ها قراردادی هیچ گاه طبقه بندی نشده اند در سیستم های رایانه ای هم وضع تقریبا به همین منوال است – یک فایروال که فقط به طور مثال دو راه ورودی خانه را بشناسد و آنها را حفاظت می کند اگر دزدی یا پکتی از راه سومی وارد شود- نتیجه چیست - در های پشتی بر روی سیستم ها نصب می شوند که نه از دیواره آتش کاری بر می آید ونه از IDS و غیره تنها راه راه شناساییManual هست ولی آیا می توان Trace های هکر را که از راه های غیر معمول وارد شبکه اتان شده است را به همین راحتی

از طریق دستی کشف و پیدا کرد به فرض چنین هکر خبره ای بخواهد یک برنامه در پشتی بر روی سیستم اتان نصب کند آیا به طوری این عمل را انجام می دهد که با مراجعه با آن مدخل ها قادر هستید که آنها را شناسایی کنید .آین همان جنگ سایبری است که هم اکنون در جریان است

برای مثال در این زمینه فقط به یک اشاره ای کوتاه اکتفا خواهم نمود :

بیشتر در های پشتی بدون استفاده از پورت در اصل از پروتکل هایی بهره می گیرند که نیازی به ارتباطات از طریق پورت ندارند یکی از پروتکل ها مرتبط به این موضوع ما عبارتست از (Internet Control Message Protocol) ICMP این یکی از بهترین پروتکل های محبوب کلاه مشکی ها برای حمل برنامه های Backdoor اشان میباشد

تعریف علمی ICMP

ICMP Definition

Internet Control Message Protocol (ICMP)

Data sent to a remote computer often travels through one or more routers; these routers can encounter a number of problems in sending the message to its ultimate destination. Routers use Internet Control Message Protocol (ICMP) messages to notify the source IP of these problems. ICMP is also used for other diagnosis and troubleshooting functions.

The most common ICMP messages are listed here. Quite a few other conditions generate ICMP messages but their frequency of occurrence is quite low.

- `Echo Request` and `Echo Reply`— ICMP is often used during testing. When a technician uses the `ping` command to check connectivity with another host, he is using ICMP. `ping` sends a datagram to an IP address and requests the destination computer to return the data sent in a response datagram. The commands actually being used are the ICMP `Echo Request` and `Echo Reply`.
- `Source Quench`— If a fast computer is sending large amounts of data to a remote computer, the volume can overwhelm the router. The router might use ICMP to send a `Source Quench` message to the source IP to ask it to slow down the rate at which it is shipping data. If necessary, additional source quenches can be sent to the source IP.
- `Destination Unreachable`— If a router receives a datagram that cannot be delivered, ICMP returns a `Destination Unreachable` message to the source IP. One reason that a router cannot deliver a message is a network that is down because of equipment failure or maintenance.
- `Time Exceeded`— ICMP sends this message to the source IP if a datagram is discarded because TTL reaches zero. This indicates that the destination is too many router hops away to reach with the current TTL value, or it indicates router table problems that cause the datagram to loop through the same routers continuously.

یک مثال از این پروتکل همان Ping خودمان است در واقع یکی از انواع ارسال نوع داده ها Echo است که در فرمان Ping استفاده می شود نوع دیگر پکت داده ICMP Quench Message است اگر بدانید اصولا Ping برای آگاهی از On بودن دیگری و Quenchبرای درخواست کاهش سرعت ارسال داده ها و همچنین ICMP Time Stamp Messages جهت آگاهی از زمان در سیستم خارجی است

بیشتر وارد جزییات نمی شوم به این دلیل که بحث بر روی این موارد به تجربه بسیار بالایی در TCP/IP نیاز خواهد داشت ولی برای آشنایی بیشتر چیزی که پروتکل ICMP را از دیگر پروتکل ها برای حمل دستورات و برنامه های در پشتی متمایز می

کند همان عدم وابستگی به سیستم TCP-UDP پورت است چون مطلب اصلی در این سیستم شناسایی و کاربرد اختلاف در منبع و همچنین مقصد ارتباطات می باشد حال آنکه ICMP فاقد چنین سیستم شناسایی است از جمله ابزار معروف در این زمینه می توان به Fportو TCPView اشاره نمود
دومین مزیتی که شاید بیشتر هکر ها به سوی در های پشتی مبتنی بر ICMP روی می آورند آنست که بسیاری و تقریبا همه شبکه های سراسر دنیا اجازه انتقال ارتباطات و پیغام های ICMPرو از میان دیواره های آتش خودشون را می دهند وبیشتر برروی ارتباطاتو ترافیک داده های TCP/UDP حساس هستند به طور مثال در شبکه ای که بسیاری از ارتباطات مثل TCPدر telnet بلوکه یا کنترل می شوند به راحتی می توانید جواب های ping را دریافت کنید در این لحظه هکر می تواند با ارسال ICMP Echo Reply Message با در پشتی نصب شده بر روی سیستم هدف از روی دیواره آتش ارتباط برقرار کند

بحث بر روی این مسائل یک مقدار پیچیده است کسانی بهتر می توانند این مفاهیم را به خوبی درک کنند که دارای پایه قوی ای در زمینه TCP-IP باشند شاید در بیشتر جا ها شنیده باشید که هکران خبره به دو چیز احاطه کامل دارند یکی مبانی شبکه به معنای واقعی کلمه که در آن غرق شده اند و دیگر programming در بیشتر زبان ها خوب مثل همه دیگر مفاهیم بعد از آن ابزار هایی بو جود می آید برای برقراری ارتباط با در های پشتی نصب شده از طریق پروتکل ICMP دو ابزار معروف در دسترس است یکی معروف است به lokiو دیگری 007Shell این ابزار پیغام ها را از طریق ICMP انتقال می دهند یک نفوذ گر می تواند با تنظیم تونل ICMP شل را حتی از طریق GUI دریافت کند ابزار های فوق را می توانید از packetstormsecurity دریافت کنید
البته انواع دیگری هم در زمینه در های پشتی بدون پورت TCP-UDP نیز قابل بحث است به علت خارج بودن از سطح علمی این مقاله با آنها نمی پردازم فقط به این مسئله واقف باشید که به صرف کنترل پورت هایتان در امان نخواهید ماند البته نفوذ یک هکر از چنین راه های پیچیده ای یک مقدار بعید است و البته باید برای ان همه زحمتی که یک هکر به خود می دهد به اطلاعات در خور توجهی دست یابد تا آنجا که من به خاطر می اورم چنین روش های به تعداد بسیار معدودی از جمله هک NASA و سکیوریتی فاکوس صورت گرفته است اکثر هک ها و نفوذ های رایج از همان پروتکل های TCP-UDP استفاده می کنند

ابزار های GUI مورد استفاده در ایجاد و نصب درب های پشتی

با استفاده ار برنامه NetCat مشاهده کردید که با استفاده از سطر فرمان به در پشتی اتصال پیدا می کردید و از آنجا به دیگر منابع دسترسی پیدا می نمودید .شاید تایپ ان همه دستورات برای بعضی ها سخت باشد و شاید هم عده ای علاقه به این موضوع داشتند که آنچه در سیستم قربانی می گذرد با چشمان خود مشاهده کنند ابزار های به عنوان Remote Control نیز دراین زمینه تهیه شدند حتما شما با بسیاری از آنها تاکنون کار نموده اید یکی از منابع خوب در زمینه پیدا کردن این ابزار ها سایت www.megasecurity.org می باشد به سایت رفته و ابزار مورد علاقه اتان را دریافت نمایید معروفترین ابزار ها در این زمینه عبارتند از :
البته باید اشاره به این موضوع کنم که بعضی از این ابزار چند منظوره هستند مثل BO2K و یا Sub7 بر خلاف تصور عموم اینها فقط ابزار های تهیه و ایجاد تروجان نیستند بلکه عمده اشخاص این ابزار ها را به خاطر این دسته از خصوصیات این ابزار می

شناسند یکی دیگر از استفاده های این گونه ابزار ها ایجاد و کنترل دسترسی به در های پشتی می باشند

Remote GUI Tools from Commercial Companies and the Computer Underground				
Tool	**Group That Released the Tool**	**Operating System Supported**	**Web Site**	**Claim to Fame**
Virtual Network Computing (VNC)	AT&T Laboratories Cambridge	Windows of all types (Win95/98/Me/NT/2000/XP/2003/CE), Various UNIX flavors, including Linux, Solaris, Macintosh, DEC Alpha Java client (which will work on any system with a Java Virtual Machine)	www.uk.research.att.com/vnc/	This free, open source ns on many kinds of ng systems, and is a e of many system strators for remote access. ers also frequently abuse it mote control backdoor.
Windows Terminal Services	Microsoft	Windows	www.microsoft.com/windows2000/technologies/terminal/default.asp	This tool is Microsoft's flagship product for remote access of a server's GUI.
Remote Desktop Service	Microsoft	Windows XP and 2003, as well as a separate client for older Windows versions	www.microsoft.com/WindowsXP/pro/using/howto/gomobile/remotedesktop/default.asp	This product is a stripped-down version of Windows Terminal Services built into newer versions of Windows.
Citrix MetaFrame	Citrix Systems, Inc.	Windows	www.citrix.com/	One of the first enterprisewide remote access tools, Citrix has gained quite a following in corporate environments.
PCAnywhere	Symantec Corporation	Windows	www.symantec.com/pcanywhere/	One of the very first tools in this category, PCAnywhere has built significant market share and remains one of the

Remote GUI Tools from Commercial Companies and the Computer Underground				
Tool	**Group That Released the Tool**	**Operating System Supported**	**Web Site**	**Claim to Fame**
				easiest tools to use.
Dameware	DameWare Development, LLC	Windows	www.dameware.com/	This commercial tool is used for remote system administration. A stripped-down free version offers a very small but full-featured free remote control client and server.
GoToMyPC	Expertcity, Inc.	Windows	www.gotomypc.com	This tool allows for remote GUI access across the Internet from any system in the world using only a browser.
Back Orifice 2000	Cult of the Dead Cow (cDc) computer underground group	Windows	www.bo2k.com	Released by the hacker group Cult of the Dead Cow, this tool is remarkably feature rich. Although it's been around a long time.
SubSeven	Mobman, programmer in the computer underground	Windows	http://packetstormsecurity.org/trojans	This is one of the most popular backdoor suites of all time.

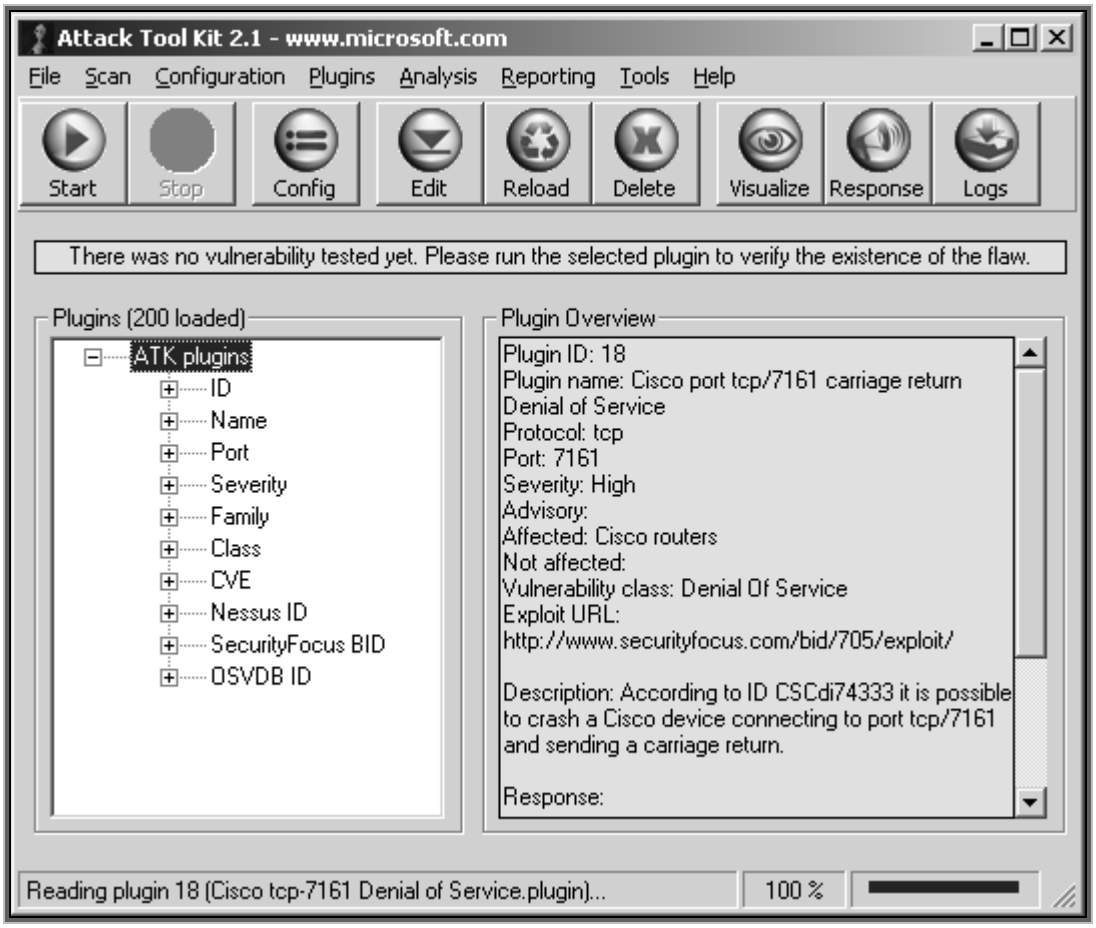
War Driving Tools For Script Kiddies

معرفی برنامه : برای بچه های شر اسکریپتی

Attack Tool kit @ www.computec.ch

لطفا از این ابزار جهت اهداف سازنده استفاده کنید و به قول خودتون جایی رو نترکونید **J**

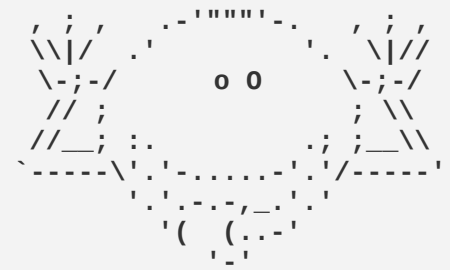

Attack Tool Kit 2.1 About
About
Project Team
Merchandising
ATK
Attack Tool Kit
Go and get your ATK shirt online!
You will find more informations about the Attack Tool Kit (ATK) on the project web site
http://www.computec.ch/projekte/atk/


Attack Tool Kit 2.1 - www.microsoft.com
File Scan Configuration Plugins Analysis Reporting Tools Help
Start
Stop
Config
Edit
Reload
Delete
Visualize
Response
Logs
There was no vulnerability tested yet. Please run the selected plugin to verify the existence of the flaw.
Plugins (200 loaded)
ATK plugins
ID
Name
Port
Severity
Family
Class
CVE
Nessus ID
SecurityFocus BID
OSVDB ID
Plugin Overview
Plugin ID: 18
Plugin name: Cisco port tcp/7161 carriage return Denial of Service
Protocol: tcp
Port: 7161
Severity: High
Advisory:
Affected: Cisco routers
Not affected:
Vulnerability class: Denial Of Service
Exploit URL:
http://www.securityfocus.com/bid/705/exploit/
Description: According to ID CSCdi74333 it is possible to crash a Cisco device connecting to port tcp/7161 and sending a carriage return.
Response:
Reading plugin 18 (Cisco tcp-7161 Denial of Service.plugin)...
100 %

Author : C0nN3ct0r ® (C0llect0r)

E-mail : C0llect0r@Spymac.com – B0rn2h4k@yahoo.com

Developed In : Black_Devils B0ys Digital Network Security Group
CopyRight © : 2005-2006 - FHS Team H4|<3rs
Researchs By : C0nN3ct0r With Cooperation of Smurf Hacker from Brazil
Special TNX 2: P0FN0R – N0thing – Sp00f3r – St0rmBit
& (s0-Mi-B34-U-t1-full-GF-N4Z1)



EVERYTHING THAT HAS A BEGINNING HAS AN END