netcat

Shabgard – Satanic Hell

By: Satanic Soulful

Satanic Hell

جهنم شیطانی

NETKAT

مباحثی پیرامون نتکت

نویسنده:Satanic Soulful
تاریخ: 29/1/1384

Contact:
Satanic.soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Special TNX♥2:
Hell Hacker – **B0rn2h4k –** S hahro Z – XshabgardX - Im4n & Y4hoO Emperor

ملاحضات:

لازم به تذکر است کلیه مطالب گفته شده تنها جنبه آموزشی دارد و هر گونه استفاده غیر آموزشی به عهده خود کاربر می باشد و نویسنده این مقاله و مدیریت سایت شبگرد و جهنم شیطانی هیچ گونه مسولیتی نسبت به استفاده نادرست از این مقاله را برعهده نمی گیرند!

استفاده از مطالب این مقاله با ذکر نام نویسنده و همچنین گروهای مربوط بلامانع است.

منابع:

Hacker’s Culb - Black Hat Hacker -@tstake -Hobbit

به نام خدای هکرها

مقدمه:
در دنیای مجازی ما هر روز ابزارهای گوناگونی درست میشود و هر کدام برای کار خاصی ایجاد میشود.
در دنیای تاریک وسیاه هکرها یکی از این ابزارها نتکت یا گروبه شبکه می باشد که به آن لقب چاقوی همه کاره و ... داده اند.
این نرم افزار کوچک و قدرتمند صاحب چنان آوازه ای شده است که به ندرت متخصص شبکه یا هکری را میتوان یافت که از این نرم افزار استفاده نکرده باشد!
اگر یک هکر تنها قادر به انتخاب یک نرم افزار برای نفوذ باشد مطمینن این نرم افزار نتکت خواهد بود زیرا دارای حجم کم و قدرت بسیار می باشد.
این نرم افزار همیشه در بهترین رده های ابزارهای امنیتی قرار دارد.
طبق گزارش یک بررسی از سویinsecure.Org در سال 2000 به منظور تعیین بهترین ابزار های امنیتی نتکت رده دوم را به خود اختصاص داد .
همینطور در سال 2003 در رده سوم جا گرفت وتا امسال بین 10 ابزار برتر امنیتی قرار گرفته است.
نتکت یکی از ابزارهای است که تحت چند سیستم عامل محبوب وجود دارد.

نت کت چیست ؟

نتکت یا گربه شبکه نرم افزاری است که قادر است داده ها را از روی شبکه ازطریق اتصالات Tcp وUdpخوانده یا بنویسد.
نتکت میتواند به عنوان پویشگر پورت و BackDoor,Port Redirector,Port Listener, Banner Grabberو..عمل کند.
البته بهترین ابزار برای این کارها نمی باشد ولی این مزیت را دارد که همه قابلیت های بالا را دارا می باشد.
نتکت به صورت ابزاری مطمین برایBack-Endطراحی شده است به طوریکه میتواند مستقیما وبه سادگی توسط برنامه های دیگر واسکریپتها اجرا شود و مورد استفاده قرار گیرد.
نتکت ابزار بسیار جالبی است که کاربردهای گوناگونی دارد مثله شناسایی شبکه واشکال زدایی آن به طوری که میتواند هر گونه اتصال مورد نظر کاربر را ایجاد کند.
نتکت توسط شرکت Hobbit و برای سیستم عامل یونیکس طراحی شده بود و در سال 1996 منتشر شد.
یول به لطف تیم کلاه سیاه لافت این نرم افزار برای خانواده ویندوز هم طراحی شد و به بازار عرضه گردید.

اگر به خواهیم به طور جامع ویژگیهای نتکت را بگویم میتوانیم به این موارد اشاره کنیم :

امکان بر قراری اتصال ونیز قبول اتصال بر رویTCP و UDP
بررسی کامل ارسال و معکوس ارسالهDNS
امکان استفاده از هر پورت مبدا
امکان استفاده از هر آدرس شبکه مبدا
قابلیت پویش پورت به صورت توکار همراه با تولید کننده اعداد تصادفی
قابلیت خواندن پارامترهای خط فرمان
حالت ارسال کند به صورت یک خط درN ثانیه
امکان اجازه به سایر برنامه ها برای سرویس دهی به ترافیک ورودی

کامپایل NetCat

کامپایل کد اصلی نتکت بسیار آسان است کافی است با نگاهی به فایل MakeFileنـوع سیستم خود را تشخیص داده ودستور<Make <systypeرا صادر کنید.
و فایل اجرای نتکت ظاهر میشود.
اگر درقسمت نوع سیستم گزینه مناسبی پیدا نکردید میتوانید گزینه Generic را انتخاب کنید.

نصب نتکت

در ویندوز نیازی به نصب نتکت نمی باشد
ولی با استفاده از فایل اجرای Nc.exeقابل اجرا می باشد.

از آدرس زیر میتوانید نتکت را دانلود کنید:
Http://atstake.com/research/tools/network_utilities

شما باید Nc رو با نوشتن "Gaping-Security-Hole" ترجمه کنید .
این هم کدهای اوون قسمت از Nc که مربوط به
توضیحاتی که دادم میشه

```
If netcat is compiled with -DGAPING_SECURITY_HOLE, the -e argument
specifies a program to exec after making or receiving a successful
connection. In the listening mode, this works similarly to "inetd" but
only for a single instance. Use with GREAT CARE. This piece of the
.code is normally not enabled; if you know what you're doing, have fun
This hack also works in UDP mode. Note that you can only supply -e
with the name of the program, but no arguments. If you want to launch
something with an argument list, write a two-line wrapper script or
.just use inetd like always
                                                        : loadports */
set "to be tested" indications in BLOCK, from LO to HI.  Almost too small

                                    /* ...to be a separate routine, but makes main() a little cleaner
==========================================================
                                                (void loadports (block, lo, hi
                                                        ;char * block
                                                         ;USHORT lo
                                                         ;USHORT hi
                                                                  }
                                                         ;USHORT x

                                                           (if (! block
                                                ;("!?bail ("loadports: no block
                                                        ((if ((! lo) || (! hi
                                        ;(bail ("loadports: bogus values %d, %d", lo, hi
                                                             ;x = hi
                                                } (while (lo <= x
                                                  ;block[x] = 1
                                                       ;--x
                                                           {
                                                 /* loadports */ {

                                                ifdef GAPING_SECURITY_HOLE#
                                /* /* global ptr to -e arg                 char * pr00gie = NULL;
                                                        ifdef WIN32#
                                BOOL doexec(SOCKET  ClientSocket);  // this is in doexec.c
                                                            else#
```

```
: doexec */
fiddle all the file descriptors around, and hand off to another prog.  Sort
of like a one-off "poor man's inetd".  This is the only section of code
.that would be security-critical, which is why it's ifdefed out by default
Use at your own hairy risk; if you leave shells lying around behind open
/* !!listening ports you deserve to lose
(doexec (fd
;int fd
}
;register char * p

/* /* the precise order of fiddlage                dup2 (fd, 0);
ifdef WIN32#
;(closesocket (fd
else#
/* /* is apparently crucial; this is                close (fd);
endif#
/* ."/* swiped directly out of "inetd                dup2 (0, 1);
;(dup2 (0, 2
/* [/* shorter argv[0                p = strrchr (pr00gie, '/');

(if (p
;++p
else
;p = pr00gie
((Debug (("gonna exec %s as %s...", pr00gie, p
;(execl (pr00gie, p, NULL
/* .../* this gets sent out.  Hmm        bail ("exec %s failed", pr00gie);
/* doexec */ {
endif#
/* endif /* GAPING_SECURITY_HOLE#
==========================================================
```

پارامتر های nc

برای به دست آوردن لیست پارامتر های nc می‌نویسیم:

```
nc -help
```

و جواب می‌شنویم:

```
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s]
[ports] ...
listen for inbound:     nc -l -p port [options] [hostname]
[port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
```

```
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

لیست پارامتر های**NC**به زبان فارسی را در پایین مشاهده می کنید.

↓▼↓

-d	بعد از اجرای برنامه‌ی Netcat کنسول آزاد می‌شود.
-e	برنامه‌ی ثانویه‌ای را اجرا می‌کند (اگر Netcat با -DGAPING_SECURITY_HOLE کامپایل شده باشد).
-i	زمان فاصل را تنظیم می‌کند. معمولا وقتی یک فایل به عنوان ورودی استاندارد مورد استفاده قرار می‌گیرد از این گزینه برای ایجاد فاصله زمانی بین دو سطر متوالی استفاده می‌شود.
-l	Netcat را وادار می‌کند که به یک اتصال ورودی گوش دهد.

-L	Netcat را با همان پارامترهایی که برای ایجاد اتصال به کار رفته بود، دوباره اجرا می‌کند. بدین ترتیب امکان برقراری اتصال بیش از یک‌بار به یک پردازه Netcat امکان‌پذیر است.
-n	Netcat تنها آدرس‌های IP عددی را قبول می‌کند و هیچ‌گونه DNS Lookup انجام نمی‌دهد.
-o	یک فایل Hex از داده‌های مبادله شده در هر دو جهت تهیه می‌کند. سطرهای فایل با دو علامت < و > به‌ترتیب به نشانه به سمت شبکه، و از شبکه نشانه‌گذاری می‌شوند.
-p	برای برقراری اتصال خارجی نیاز است و پورت مورد نظر را مشخص می‌کند. به هنگام گوش دادن به اتصال ورودی نیز پورت مورد نظر را مشخص می‌کند.
-r	موجب می‌شود پویش پورت‌ها به صورت تصادفی انجام گیرد. همچنین برای انتخاب پورت مبدا به صورت تصادفی نیز به کار می‌رود.
-s	برای تعیین آدرس IP مبدا استفاده می‌شود.
-t	اگر Netcat با گزینه DTELNET- کامپایل شده باشد، انتخاب این پارامتر به هنگام اتصال به سرویس‌دهنده Telnet باعث می‌شود تا مذاکرات اولیه به صورت اتوماتیک انجام شود.
-u	برای برقراری اتصال UDP به جای TCP مورد استفاده قرار می‌گیرد.
-v	میزان اعلان جزئیات اتصال را افزایش می‌دهد.
-w	تعداد تلاش برای برقراری اتصال را محدود می‌کند.
-z	مانع از ارسال هر گونه داده به اتصال TCP می‌شود. در اتصال UDP نیز داده‌های بسیار محدود، تنها برای کاوش ارسال می‌شود. اصولا در پویش پورت و تنها به منظور تعیین پورتهای باز از این پارامتر استفاده می‌شود.

اگر هیچ گونه پارامتری به کار نرود نتکت از ما تقاضای پارامتر میکند و آماده دریافت آن از طریق ورودی استاندارد خواهد بود.
بعد از دریافت یک سطر وردی آن را به پارامترهای تشکیل دهنده شکسته ومورد پردازش قرار می دهد.
یکی از مزیت های این روش مخفی نگه داشتن پارامتر دستور اجرا شده از چشم Psمی باشد.
میزبان می تواند به هر دو صورت اسم یا آدرس ذکر شود.

اگر Nc –n به کار گرفته شود
نتکت تنها آدرس های آی پی را به صورت عددی قبول میکند.
بنابراین هیچ گونه DNS Loockupصورت نمگیرد.
و اگر Nc -v به کار گرفته شود
نتکت به طور کامل هر دو گونهLoockupمستقیم وبر عکس اسم وآدرس را برای میزبان انجام میدهد ودر صورت عدم تطابق نام ها درDNSپیغام خطای نمایش داده میشود.
برای برقرای اتصال به خارج(OutBound)بایستی پورت مقصد ذکر شود. پورت مقصد نیزمیتواند به صورت عددی یا اسمی درج شود.
به طور کلی سویچ v-میزان اطلاعات جزئیات را مشخص می کند این سویچ باعث میشود کاربر اطلاعاتی در مورد اتصال جاری دریافت کند.
استفاده از این سویچ به صورت پشته سر هم (v- v-)باعث میشود که نتکت اطلاعات بیشتری به کاربر بدهد

سوییچNc -w
با استفاده از این سویچ میتوانید زمان لازم برای برقراری یک اتصال را کاهش دهید.
استفاده از این سویچ به شکلnc –w 3 همراه با سویچv- بسیار

معمول است و عملی همانند تلنت را انجام میدهد.

سوییچ u-

با استفاده از این سوییچ به جای اتصال به Tcpاتصال udp برقرار خواهد شود البته به خاطر اینکه udp پروتکل اتصال نمی باشد نتکت از مکانیزمUdp Socket Connected که توسط بسیاری از کرنل ها پشتیبانی میشود به منظور برقراری ارتباطudp استفاده می کند.
هنگام اتصال udp عملا تا زمان خواندن از ورودی استاندارد چیزی ازسال نمی شود و نتکت پورت udpرا پورت باز(Open Port) فرض میکند.
در بعضی مواقع با استفاده از این کار می توان فهمید آیا در طرف دیگر سرویس دهنده ای در حال سرویس دادن است یا نه؟!

سوییچNc –o logfile

برای بدست آوردن لیستی از داده های مبادله شده به زبان هکس(Hex) از این سوییچ استفاده میکنیم.
سطرهای فایل با< و > به ترتیب به سمت شبکه واز شبکه نشانه گذاری میشود.
ذخیره اطلاعات مبادله شده باعث کندی عمل و سرعت نتکت میشود بنابراین در مواردی که سرعت خیلی مهم می باشد از این گزینه استفاده نکنید تا باعث کندی عمل نشود
نتکت میتواند به راحتی به همه پورت ها(حتی اگر آن پورت در حالت سرویس دهی باشد) ضمیمه شود.

سوییچ p-

نتکت پورت را به طور پیش فرض ندارد و برای دادن پورت به نتکت از سوییچp- استفاده میکنیم
به این عمل اصطلاحا عمل تعیین سوکت نیز گفته میشود.

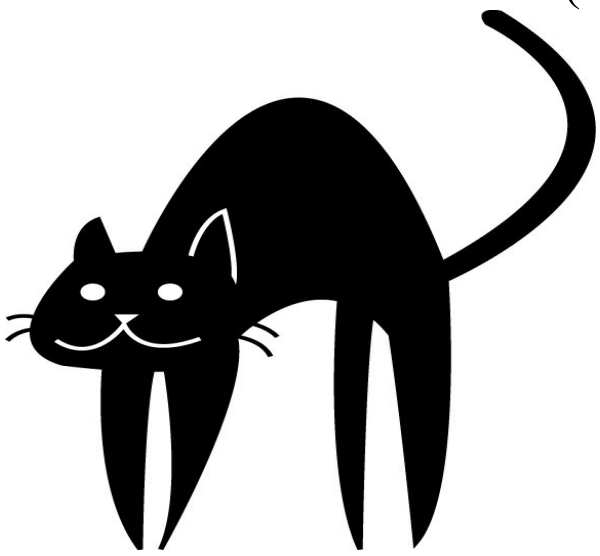
کاربران با بیشترین حد دسترسی(Root)
میتوانند هر پورتی استفاده نشده ای را حتی زیر 1024 را به عنوان پورت مبدا انتخاب کنند.
استفاده از این سوییچ باعث میشود که پورت مبدا توسط سیستم عامل و از بین پورت های استفاده نشوده تعیین گردد(مگر اینکه از سوییچ r– استفاده شود)

در وضعیت گوش دادن (Listening)نتکت منتظریک اتصال مانده وسپس تبادل داده ها را انجام میدهد.
بنابراین با استفاده از Nc –l –p 1234 <filename وقتی کسی به پورت 1234 وصل شود فایل مزبور برایش فرستاده میشود.
وضعیت گوش دادن عموما با پارامترهای محلی استفاده میشود
اگر در وضعیت گوش دادن میزبان مقصد و پورت محلی را تعیین کند نتکت تنها از میزبان و پورت مشخص شده اتصالات را قبول میکند وبقیه اتصالات را رد خواهد کرد.

اگر از سوییچv-
استفاده کنیم نتکت با دریافت هر تقاضا برای اتصال ,آدرس و پورت متقاضی را ثبت خواهد کرد.
در حالت معمول وقتی یک اتصال توسط نتکت دریافت شود و به پایان رسید کار نتکت خاتمه پیدا میکند.

سوییچL-
برای برقرار کردن چندین اتصال متعدد از این سوییچ استفاده میکنیم و باعث میشود که در یک لحظه چندین اتصال برقرار باشد.
وقتی کار یکی از اتصال ها خاتمه پیدا کرد نتکت به طور اتوماتیک با استفاده ازپارامترهای قبلی اجرا شده و منتظر دریافت اتصال جدیدی می شود

اگر نتکت باDGAPING_SECURITY_HOLE– کامپایل شده باشد سوییچE- برنامه ای را مشخص میکند که بایستی بعد از دریافت یک اتصال موفق اجرا شود کارکرد این گزینه در وضعیت گوش دادن همانندintedمی باشد.
با این تفاوت که بدین طریق فقط یک برنامه می تواند اجرا شود.
بنابراین باید مواظب این قسمت بود زیرا ...!!؟
این قطعه کد در حالت عادی فعال نیست و اگر شما از کاری که میکنید مطمئن هستید!پس از آن لذت ببرید ☻
دقت کنید که تنها اجرای برنامه ای مورد نظر بدون ارسال هیچ گونه پارامتری میسر خواهد بود.
پس اکر قصد اجرای برنامه ای با پارامتر را دارید از یک فایل دسته ای یا اسکریپت استفاده کنید.
اگر نتکت باDTLENET- کامپایل شده باشد
سوییچT- امکان پاسخ گویی به گزینه های تلنت را فراهم می کند.
بدین وسیله نتکت میتواند به سرویس دهنده ای تلنت وصل شود و را مذکرات اولیه تا رسیدن بهLogin انجام بدهد
به دلیل آنکه توان تغییر جریان را دارد به طور پیش فرض فعال نمی باشد(با توجه به اطلاعات کاربراگر لازم باشد کاربر می تواند این گزینه را فعال کند)



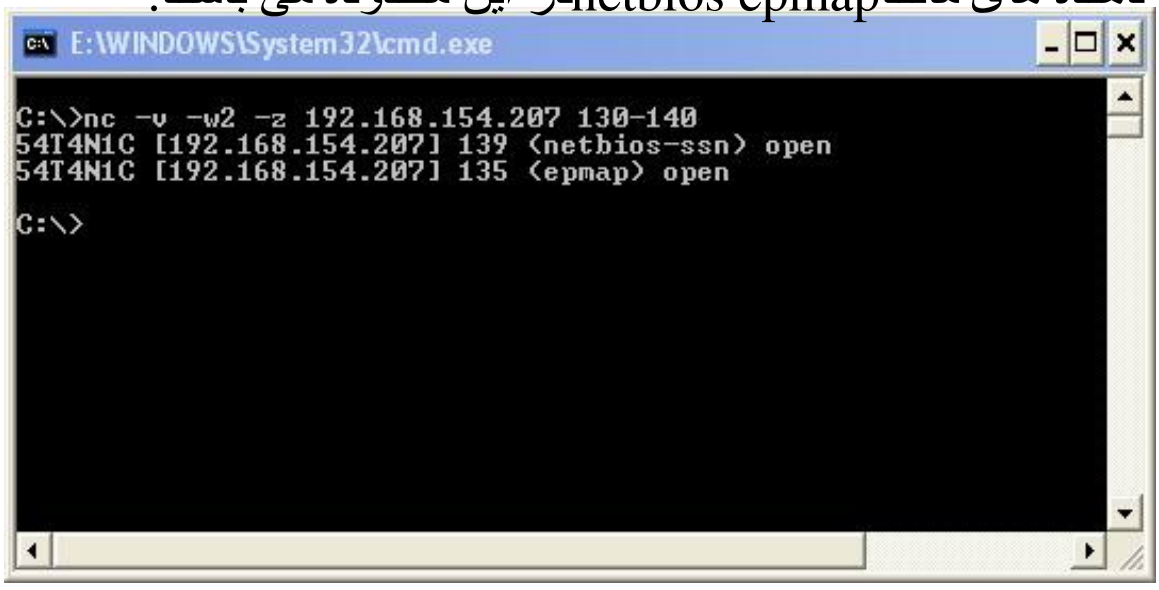
داده های که از شبکه دریافت می شود همیشه با بیشترین کارایی در بسته های 8 کیلو بایتی به خروجی استاندارد تحویل داده میشود.
ورودی استاندارد نیز به این صورت به شبکه ارسال می شود ولی سوییچi-فرجه زمانی را تعیین میکند که سرعت ارسال را به طور قابل توجهی کاهش میدهد.

پویش پورت یا اسکن پورت

پویش پورت روش متدوالی برای کشف دنیای خارج می باشد نتکت پارامترهای خود را به این صورت میگیرد:
ابتدا سوییچ,سپس آدرس میزبان و مقصد و هر چیزی که بعد از اینها بیاید به عنوان نام یا شماره پورت تعبیر می شود که می تواند به شکل محدوده ای از پورت به فرمm-n نیز درج شود. اگر بیش تر یک پورت مشخص شده باشد نتکت به تمام آنها به ترتیب وصل می شود و به همه آنها داده های یکسانی را می دهد.
ذکر بیش از یک پورت مقصد باعث توقف ارسال می شود وپیام خطای صادر میشود.
برای انجام پویش پورت بدون ارسال داده بایستی از سوییچz- استفاده شود مانند مثال زیر:

Nc –v –w2 –z target 130-140

هدف را پویش کند چون سرویس 130 تا 140سعی دارد پورت های دهنده های مانندnetbios epmapدر این محدوده می باشند.



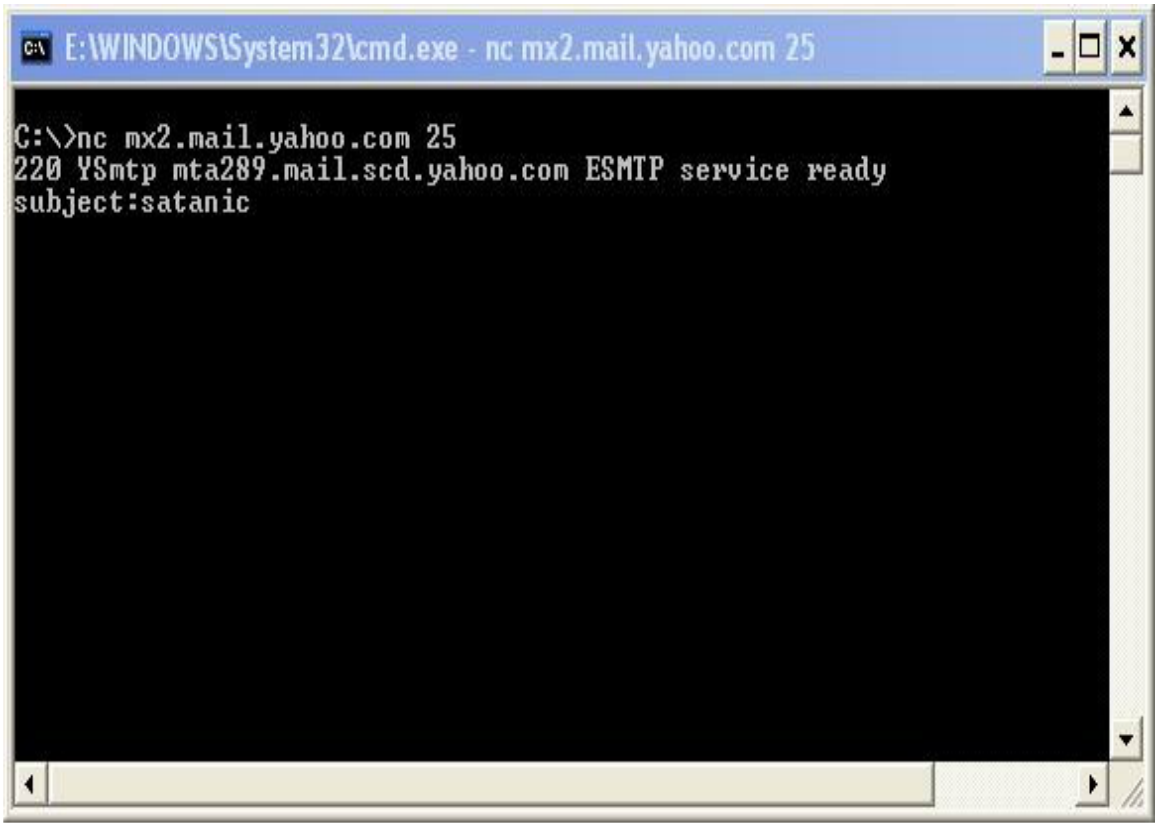
در شکل بالا پورت های از 130 تا 140 اسکن شده و جواب داده شده که پورت های 139 و 135 که به ترتیب مربوط به نت بایوز وای پی مپ می باشد باز است.
از پویش پورت در بسیاری از کارها و نفوذ ها می توان کمک کرد یکی از مهمترین دلیل های محبوبیت نتکت بین هکر ها این قابلیت می باشد.

☺

تا این صفحه بهضی از سوییچ ها و ترفندها را به شما آموختیم حالا با چند مثال بهضی از کارایی های این چاقو را برای شما می نویسیم.

استفاده از نتکت به جایTelnet

نتکت به عنوان ابزاری که قادر است باDaemonهای مختلف مکالمه کند,جانشینی خوب برای ابزار قدرتمند تلنت به حساب می آید به عنوان مثال استفاده از نتکت به شکلNc Host 25برای اتصال و مکالمه یک سرویس دهنده میل اس ام تی پی(Smtp)نه تنها بسیار ساده تر بلکه موثر تر نیز می باشد



همان گونه که می توان از تلنت به جای یکMail Bomber(FakeMail) استفاده کرد از نتکت هم می توان همان کارایی را دید.
البته این تنها یک مثال کوچک برای آشنایی بیشتر شما با این چاقوی همه کاره می باشد وکار های که شما با تلنت انجام میدهید را میتوان با این برنامه کوچک انجام داد.

پویش پورت یاPort Scaning

یکی دیگر از مزیت های نتکت پویش کننده پورت این برنامه می باشد.

این مزیت به شما کمک میکند تا پورت های هدف را درکمترین زمان پویش کرده و پورت های باز وبسته را تشخیص داد.

در اویل مقاله گفتیم:" اگر یک هکر تنها قادر به انتخاب یک نرم افزار برای نفوذ باشد مطمینن این نرم افزار نتکت خواهد بود"

اگر شما به خواهید به جای نفوذ کنید مطمینن نرم افزارهای مانند:

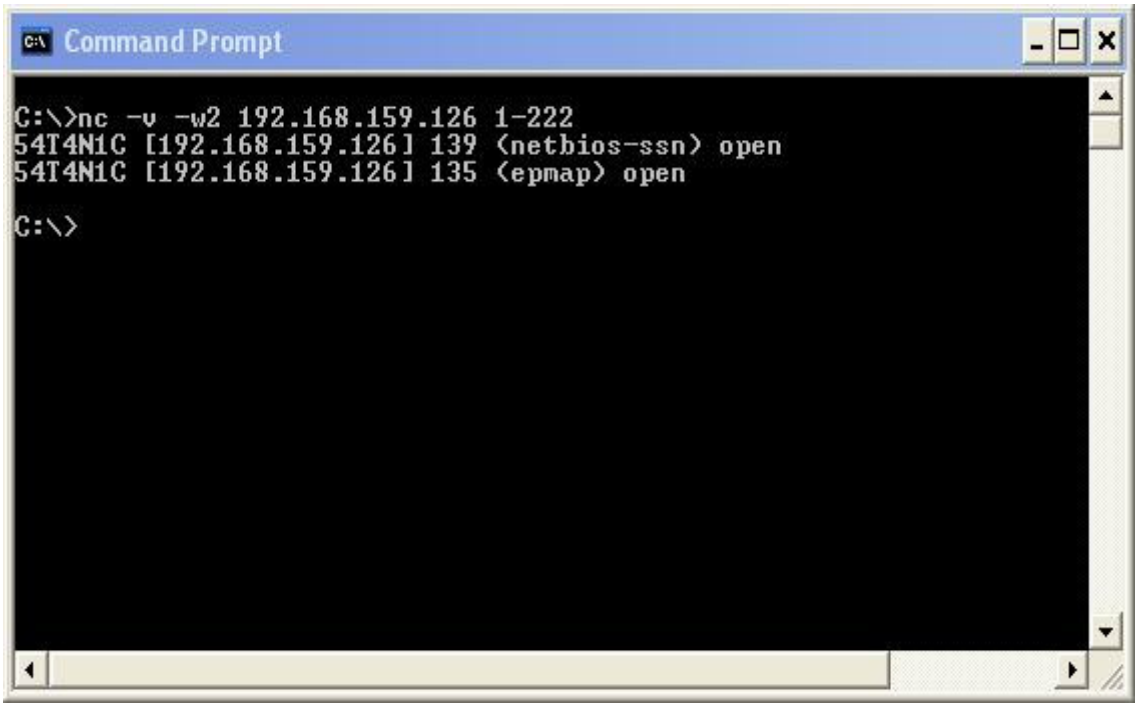
Ip Scaner , Port Scaner ,file Transfer , Script uploader ... & را لازم خواهید داشت ولی شما تنها قادر به استفاده از یک نرم افزار هستید پس بهترین وتنها ترین نتکت هست!!! ☺

برای اسکن کردن پورت ها کافیست دستور زیر را نوشته:

Nc –v –w2 Target FirstPort-EndPort

مانند مثال زیر(در مثال زیراز پورت 1 تا 222 هدف اسکن میشود!)

Nc –v –w2 192.168.159.126 1-222

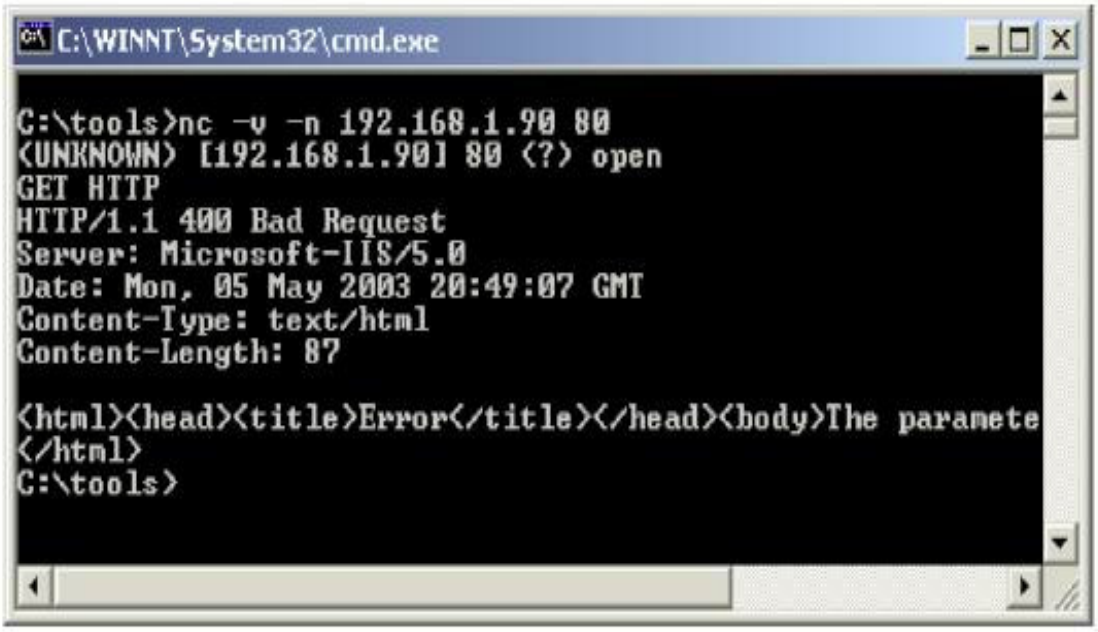


در شکل بالا میبینید که پورت های 139 و 135 پورت های باز هدف هستن.

جمع آوری Bannerهای سرویس دهنده

بعضی اوقات شده که شما به خواهید بدانید پشت بعضی پورت ها چه سرویس دهنده ای در حال کار است !؟
یکی دیگر از خصوصیات نتکت جمع آوری بنر ها است
برای این کار در خط فرمان دستور زیر را مینویسیم:
Nc –v –n Target Port Number
در مثال های زیر پورت های 21 و 80 را برای مثال به شما نشان میدهیم!
در مثال اول پورت 21 را چک میکنیم:
Nc –v –n 192.168.1.90 21

شکل بالا اطلاعاتی از پورت 21 وسرویس دهنده از پورت به ما میده
مثال دوم پورت 80
Nc –v –n 192.168.1.90 21



در شکل بالا پورت 80 نیز بررسی شود.
ما فقط برای مثال این 2 پورت را گفتیم شما میتوانید هر پورتی را چک کنید.

سرویس دهنده وب

از نتکت می توان به عنوان یک سرویس دهنده ساده وب استفاده نمود.
کافیست فقط پاسخHttpرا در اول فایلHtmlخود قرار دهیم .
بنابراین فایلی همانند فایل زیر درست میکنیم:

Http/1.0 200 OK
Centent-type: text/plain
Content-length: 724
<HTML>
<BODY>
.

.
.
.
</BODY>
</HTML>

و این فایل را با نامIndex.htmذخیره میکنیم.
درادامه نتکت را با فرمان زیر اجرا میکنیم.

Nc –l –p 80 < index.htm

طبق این دستور نتکت به پورت 80 گوش میدهد وبرای هر اتصالی فایل ایندکس فرستاده میشود.
این فقط یک مثال بود شما میتوانید با این کار حتی اسکریپت هم بفرستید.

Flooding شبکه

برای پر کردن شبکه از داده های بی مصرف برای کاربرد های گوناگونی استفاده میشود.
مثله چک کردن اجزای مختلف شبکه مانند مسیر یاب,سوییچ,فایروال ظرف عسل و... بسیار مفید می باشد.
برای این کار می شود از نتکت استفاده کرد:

```
yes AAAAAAAAAAAAAAA | nc –v –v –l –p 2222 > /dev/null
```

و در طرف دیگر:

```
yes BBBBBBBBBBBBBBB | nc othermachine 2222 > /dev/null
```

این کار باعث ترافیک زیادی از داده های بی مصرف آ وبی میشود استفاده از سوییچ v-باعث میشود که در پایان کار نتکت لیستی از داده های ارسال شوده را ذخیره کند.

مطمئن باشید که برای Netcat کاربردهای بسیار بیشتر از آنچه در بالا اشاره شد وجود دارد. به عنوان مثال برای کاربردهای که قبلا مورد استفاده قرار گرفته‌اند می‌توان به موارد زیر اشاره کرد: پویشگر متنی وب، انتقال فایل به دستگاهی که تنها پویشگر وب دارد، استفاده همانند inetd، رله ترافیک، port redirect، استراق سمع برنامه کاربردی، تست remote syslogger ، تست packet filter، محافظت از سرویس‌دهنده‌ی X (رابط گرافیکی لینوکس) در برابر دسترسی خارجی، ایجاد سرویس‌دهنده‌های خاص منظوره، و بسیاری دیگر که مطمئناً مستندسازی نشده‌اند. هر روز کاربردهای جدیدی با توجه به خلاقیت کاربران (و یا شاید نیاز کاربران) از این نرم‌افزار به عمل می‌آید. ویژگی‌ها و قابلیت‌های Netcat، زمانی که با قدرت برنامه‌نویسی و در حقیقت زبان اسکریپت تلفیق شود، امکانات بی‌نظیری به این برنامه خواهد داد. یک مجموعه از اسکریپتهایی که از Netcat استفاده نموده‌اند در داخل پوشه scripts/ در بسته نرم‌افزاری Netcat وجود دارد. مطالعه بیشتر این اسکریپت‌ها توصیه می‌شود.

ßLa¢k Hât Ha¢ker’s

در این ژورنال راجبه یکی از تیم های بلک هت(کلاه سیاه)ایرانی گفتم براتون بگم تا بیشتر با تیم های خوبه ایرانی آشنا شید!

Emperor Team

تیم امپراطور یکی از تیم های خوب ایرانی در عرصه کلاه سیاه ها می باشد این تیم با هک کردن بالای 2050 سایت یکی از بزرگترین تیم های دیفیس ایرانی میباشد!
این تیم که دارای 7 عضو می باشد به نام های IM4N,Y4Ho0,BuG,Cl4w,EimaN,@RASH&Turbo که مدیریت این تیم باIm4nمیباشد.

از کارهای بزرگ این تیم میتوان به برنامه های:
Ybad 1,YBad 1.5,WinNCاشاره کرد!
از سایت های معروف که توسط این تیم دیفیس شده است میتوان
سایت های :
کارخانه زمزم,آموزش پرورش کلیه مناطق تهران,گروه موزیک
آریان,کنفدراسیون تیم ملی فوتبال,دانشگاه شریف,دانشگاه آزاد قزوین
وسمنان,118 تهران,وزارت ارشاد,کمپانی رنو در ایران و ...
میتوانید با مراجعه به لینک زیر کل سایت های هک شوده را مشاهده
کنید:
http://www.zone-h.org/en/defacements/special/filter/filter_defacer=eMP3R0r+TEAM/

Im4n Emperor
آدمین این تیم که یکی از دیفیسرهای این تیم هم می باشد عضو تیم های
بزرگی همچون شبگرد وپرشین هکرز هم می باشد ☺

Im4n-Y4ho0

یکی دیگر از اعضای این گروه کامران معروف به امپراطور یاهو می باشد که یکی دیگر از اعضای تیم دیفیس امپراطور می باشد.

Lord Cracker-IranMatrix-Mohmad Shabgard-Danil-Im4n

Author: Satanic Soulful
E-Mail: Satanic.Soulful@GMail.Com
Satanic_Soulful@Yahoo.Com
Developed In:Satanic Digital Network Security ™
Special TNX 2 :Hell Hacker – Collector – S_hahroo_Z - Kami
Research By:5/-\t4N1C

For More Information Go to Http://Hack-er.cjb.net/

SATANIC
DIGITAL NETWORK SECURITY
Www.Hack-er.Cjb.Net

My Deram Is All Day For Girl Is Dark&Ominous♀