

بنام یزدان پاک

www.cyberwarez.tk



Dangerous for hackers

data ir security group present

www.datairan.ir



Packet sniffing



packet sniffing

tnx t0 :

DELL NEO

ALL Right reserved for lord sooshi4nt

ALL Right reserved for data ir security team

this book is not for professoinal men in pc and cyber world !!

pleas don't try this note in persian network !

my group web site : www.datairan.ir

my personal page : www.cyb3rwarez.tk

my e-mail : lord_sooshi4nt@cyb3rwarez.tk

my Y4Ho0 id : lord_sooshi4nt@yahoo.com

lord sooshi4nt

نویسنده / مترجم :

www.datairan.ir

صفحه وب :

www.cyb3rwarez.tk

صفحه شخصی :

lord_sooshi4nt@cyb3rwarez.tk

ایمیل :

lord_sooshi4nt@yahoo.com

آیدی یاهو :

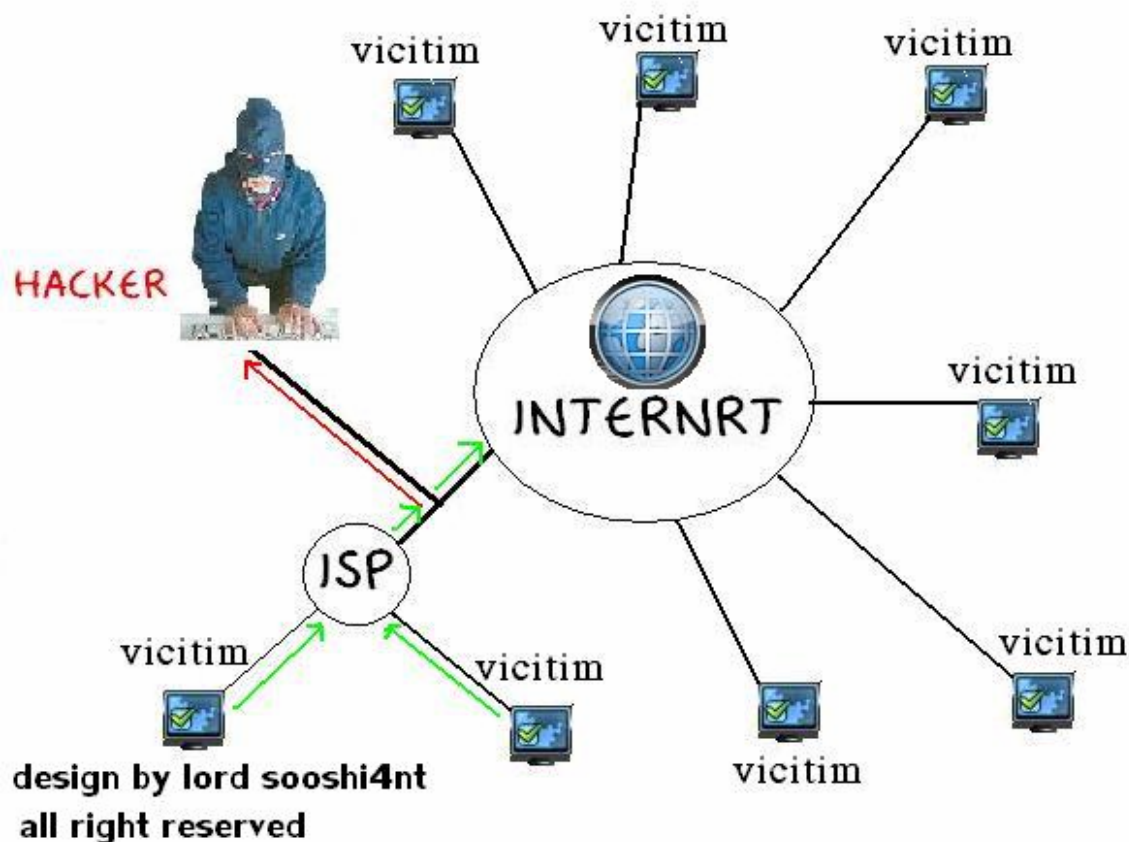
کلیه حقوق این مقاله متعلق به نویسنده آن است و هرگونه کپی برداری و یا نشر این مقاله غیر مجاز است .

اسنیفر چیست ؟

اسنیفر یک برنامه استراق سمع در شبکه است . هکر با استفاده از یک اسنیفر ، اطلاعات سرگردان بر روی شبکه (معمولا شبکه های local) را جمع آوری میکند . از آنجایی که این اطلاعات encode شده نیستند ، هیچ نیازی به شکستن یا cracking آن ها نیست . فقط با چند دقیقه sniff میتوان تمام اطلاعات از جمله username و passwordها را بدست آورد . البته در این مقاله بحث ما بصورت white paper است و قصد آموزش خرابکاری را نداریم . البته اسنیفر میتواند بصورت یک نرم افزار packet monitoring هم مورد استفاده قرار گیرد ، به این صورت که مدیران سرورها با راه اندازی اسنیفرها تمامی اطلاعات رد و بدل شده را بررسی میکنند . این کار فقط توسط مدیران باهوش سرورها انجام میگردد . یک مثال میزنم ، فرض کنید روی یک سرور نرم افزار netcat را آپلود کرده ایم و به کار transfer اطلاعات مشغول هستیم . حال مدیر آن سرور اسنیفر را راه اندازی میکند ، حالا چه اتفاقی میافتد ؟ بله ! درست حدس زدید ، شما شناسایی میشوید و تمام اطلاعات شما (بدون این که متوجه شوید و البته در دلتان هم کمی به آن ها میخندید که نتوانستند مچ شما را بگیرند!) برای مدیر نمایان میشود و پس از چند روز شما در حال آب خنک خوردن در زندان هستید ! خوب من در این مقاله در این زمینه (نصب و استفاده از اسنیفر روی سرور) بیشتر از این توضیح نخواهم داد چون از موضوع اصلی فاصله میگیریم . فقط خواستم قدرت اسنیفر ها را نشان بدهم ! ابتدا شما را با کار کردن با چند اسنیفر آشنا میکنیم . سپس نحوه ی کار اسنیفر ها و راه های مقابله با آن ها را بررسی میکنیم . پس حاشیه دیگر تمام ! بریم سر اصل مطلب !

internet protocol مسئول ارسال بسته ها بین رایانه ها میباشد و ما اطمینان نداریم که این پروتکل تضمین میکند که این اطلاعات توسط رایانه های دیگر دریافت میشود یا خیر . همان طور که میدانید انواع شبکه ها از جمله سیمی و wireless, خطوط تلفن و تلویزیون و قابل sniff هستند . زمانی که شما در حال لاگین به یک سایت هستید ، از

بین رایانه ی شما تا سرور مورد نظر مسیر طولانی طی میشود . ابتدا شما با isp ارتباط برقرار میکنید سپس به همراه تمامی کاربران به دنیای اینترنت وارد میشوید ، حالا هر کجا که میخواهید میروید . اما در این میان ذهن پلیدی وجود دارد که در حال جاسوسی بر روی شبکه است ! او با جمع آوری اطلاعات در حال عبور ، اطلاعات شما به همراه بقیه کاربران را بر روی صفحه مانیتور خود میبیند . بدون این که روح شما خبر دار شود .



همان طور که میدانید یکی از اولین اسنیفر های پیشرفته را گروه **l0pht** ایجاد است . این اسنیفر اطلاعات در حال گذر بر روی شبکه را جمع آوری میکند البته خود هکرهای این گروه اسم این کار را هک کردن نمیگذارند و فقط به آن " جمع آوری اطلاعات " میگویند ! و از اولین قربانیان این اسنیفرها دانشگاه ها و ادارات بودند . خوب ابتدا من اسنیفر مشهور **ethereal** را معرفی میکنم . این اسنیفر یک نرم افزار فوق العاده برای ضبط کردن یا همان **capture** اطلاعات سرگردان بر روی شبکه است . توسط این نرم افزار اطلاعات زیر قابل جاسوسی است :

IP addresses

Hostnames

Routes

Data (FTP , Telnet, e-mails, etc.).

Protocol information

خوب من طریقه ی نصب این نرم افزار هم در ویندوز و هم در لینوکس را توضیح خواهم داد . البته اگر از کسانی باشید که مقالات ما را میخوانید ، ما قبلا در مقالات اشاره ی کوچکی به این اسنیفر کرده بودیم .



طریقه ی نصب در لینوکس کلاه قرمز !

شما میتونید این نرم افزار رو از آدرس <http://www.ethereal.com> دریافت کنید البته حتما باید **winpcap** رو هم نصب کنید

ابتدا در دایرکتوری لینوکس این عبارت رو تایپ کنید :

```
tar -zxvf ethereal-0.10.13.tar.gz
```

خوب حالا در یک دایرکتوری جدید تایپ کنید :

```
ethereal-0.10-13
```

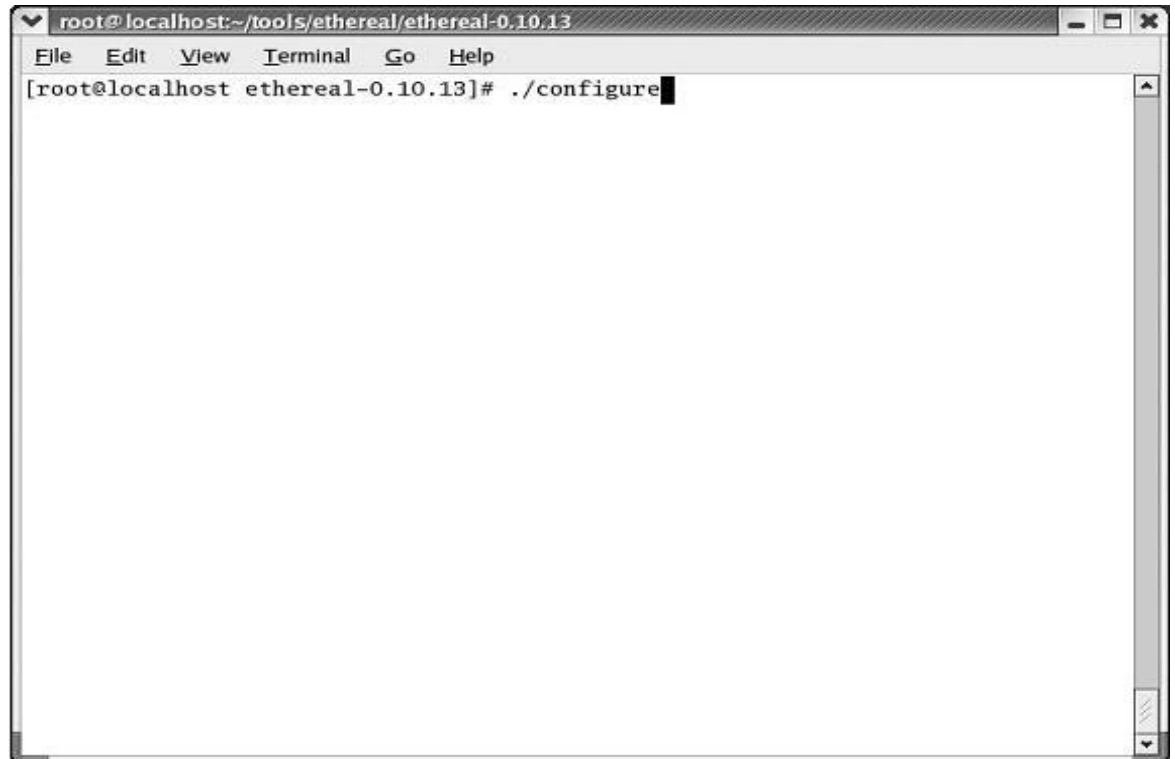
حالا ما باید دایرکتوری رو تغییر بدیم . بدین منظور تایپ کنید :

```
cd ethereal-0.10.13
```

حالا نرم افزار برای کامپایل آماده میشه . برای این کار تایپ کنید :

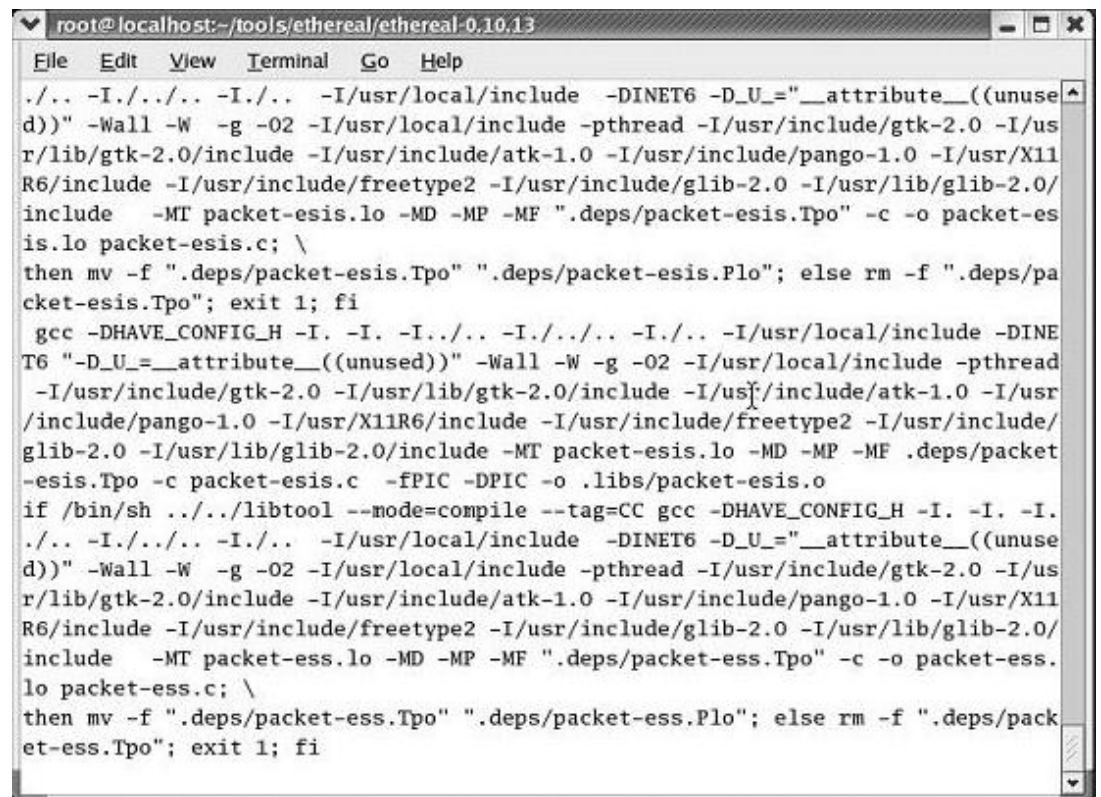
```
./configure
```

خوب حالا به تصویر زیر دقت کنید :



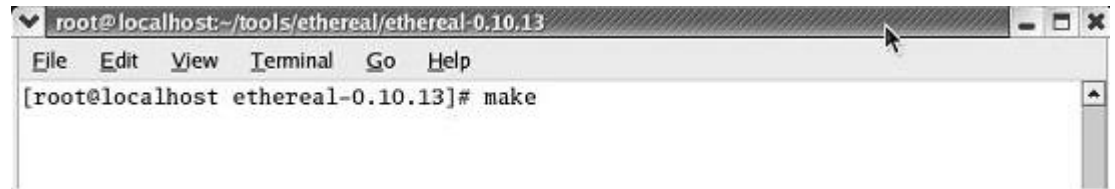
```
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
[root@localhost ethereal-0.10.13]# ./configure
```

بعد از این مرحله شما موقع کامپایل شدن میتونید چنین چیزی رو مشاهده بکنید که این مرحله حدود 10 تا 20 دقیقه طول میکشه



```
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
./.. -I./../.. -I./.. -I/usr/local/include -DINET6 -D_U="__attribute__((unused))" -Wall -W -g -O2 -I/usr/local/include -pthread -I/usr/include/gtk-2.0 -I/usr/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr/include/pango-1.0 -I/usr/X11R6/include -I/usr/include/freetype2 -I/usr/include/glib-2.0 -I/usr/lib/glib-2.0/include -MT packet-esis.lo -MD -MP -MF ".deps/packet-esis.Tpo" -c -o packet-esis.lo packet-esis.c; \
then mv -f ".deps/packet-esis.Tpo" ".deps/packet-esis.Plo"; else rm -f ".deps/packet-esis.Tpo"; exit 1; fi
gcc -DHAVE_CONFIG_H -I. -I. -I./.. -I./../.. -I./.. -I/usr/local/include -DINET6 -D_U="__attribute__((unused))" -Wall -W -g -O2 -I/usr/local/include -pthread -I/usr/include/gtk-2.0 -I/usr/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr/include/pango-1.0 -I/usr/X11R6/include -I/usr/include/freetype2 -I/usr/include/glib-2.0 -I/usr/lib/glib-2.0/include -MT packet-esis.lo -MD -MP -MF .deps/packet-esis.Tpo -c packet-esis.c -fPIC -DPIC -o .libs/packet-esis.o
if /bin/sh ../../libtool --mode=compile --tag=CC gcc -DHAVE_CONFIG_H -I. -I. -I./.. -I./../.. -I./.. -I/usr/local/include -DINET6 -D_U="__attribute__((unused))" -Wall -W -g -O2 -I/usr/local/include -pthread -I/usr/include/gtk-2.0 -I/usr/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr/include/pango-1.0 -I/usr/X11R6/include -I/usr/include/freetype2 -I/usr/include/glib-2.0 -I/usr/lib/glib-2.0/include -MT packet-ess.lo -MD -MP -MF ".deps/packet-ess.Tpo" -c -o packet-ess.lo packet-ess.c; \
then mv -f ".deps/packet-ess.Tpo" ".deps/packet-ess.Plo"; else rm -f ".deps/packet-ess.Tpo"; exit 1; fi
```

برای مرحله بعد در کامند تایپ کنید : **make** و سپس اینتر بزنید



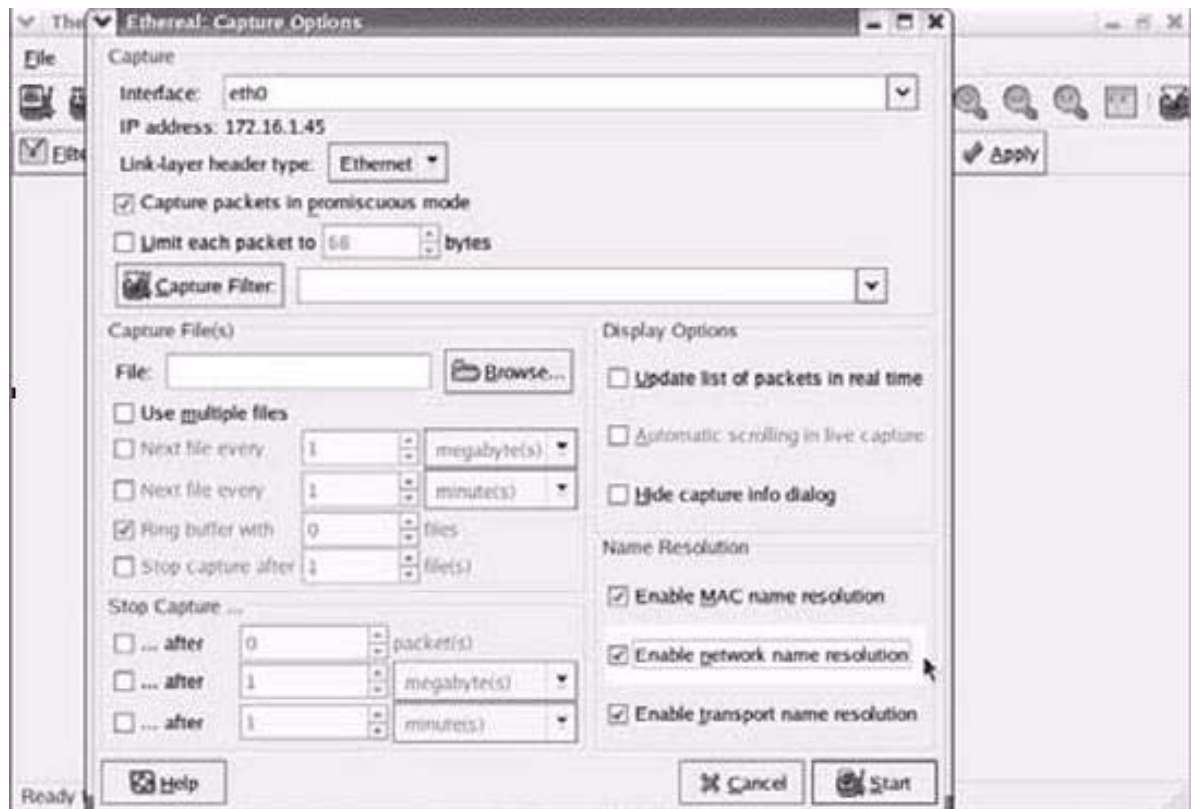
خوب بعد از این کار نرم افزار با موفقیت نصب میشه .

خوب تبریک میگم شما با موفقیت عملیات نصب رو تموم کردید . حالا وقتش رسیده کار با نرم افزار رو شروع کنیم بدین منظور در کامند تایپ کنید :

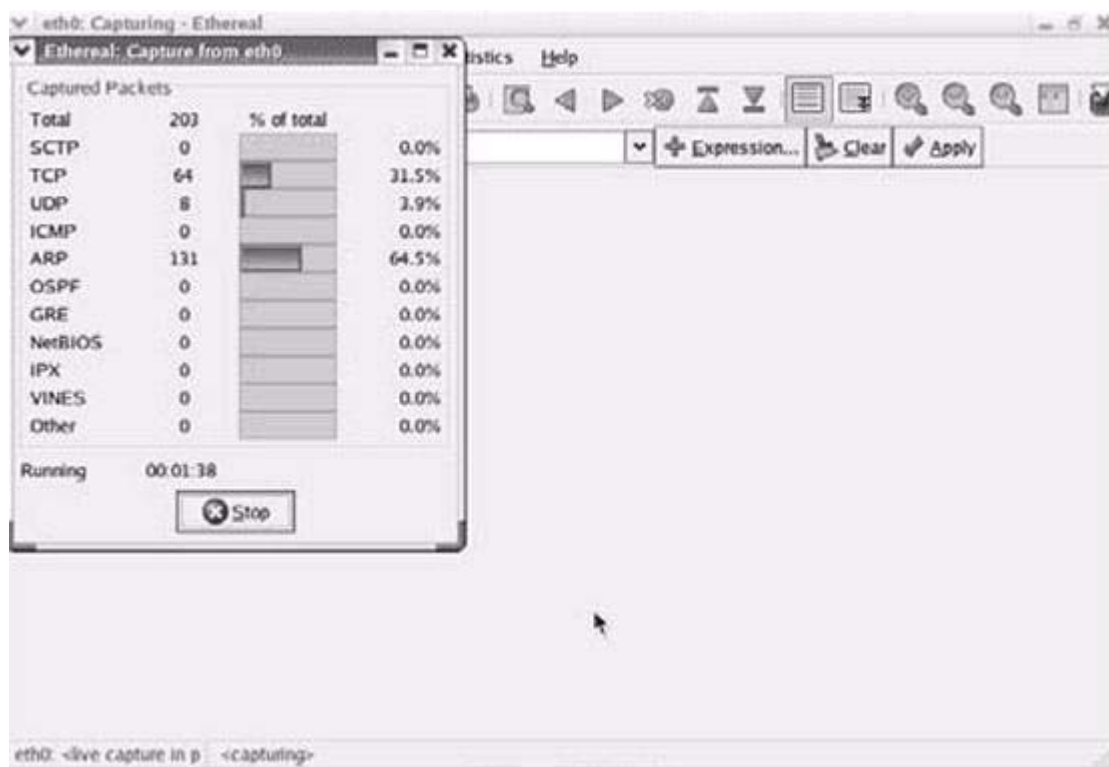
`./ethereal`

خوب حالا نرم افزار شروع به کار میکنه اما یک رابط گرافیکی داره . (دوستان برای بهتر کار کردن با نرم افزار حتما `readme` رو مطالعه بفرمایید)

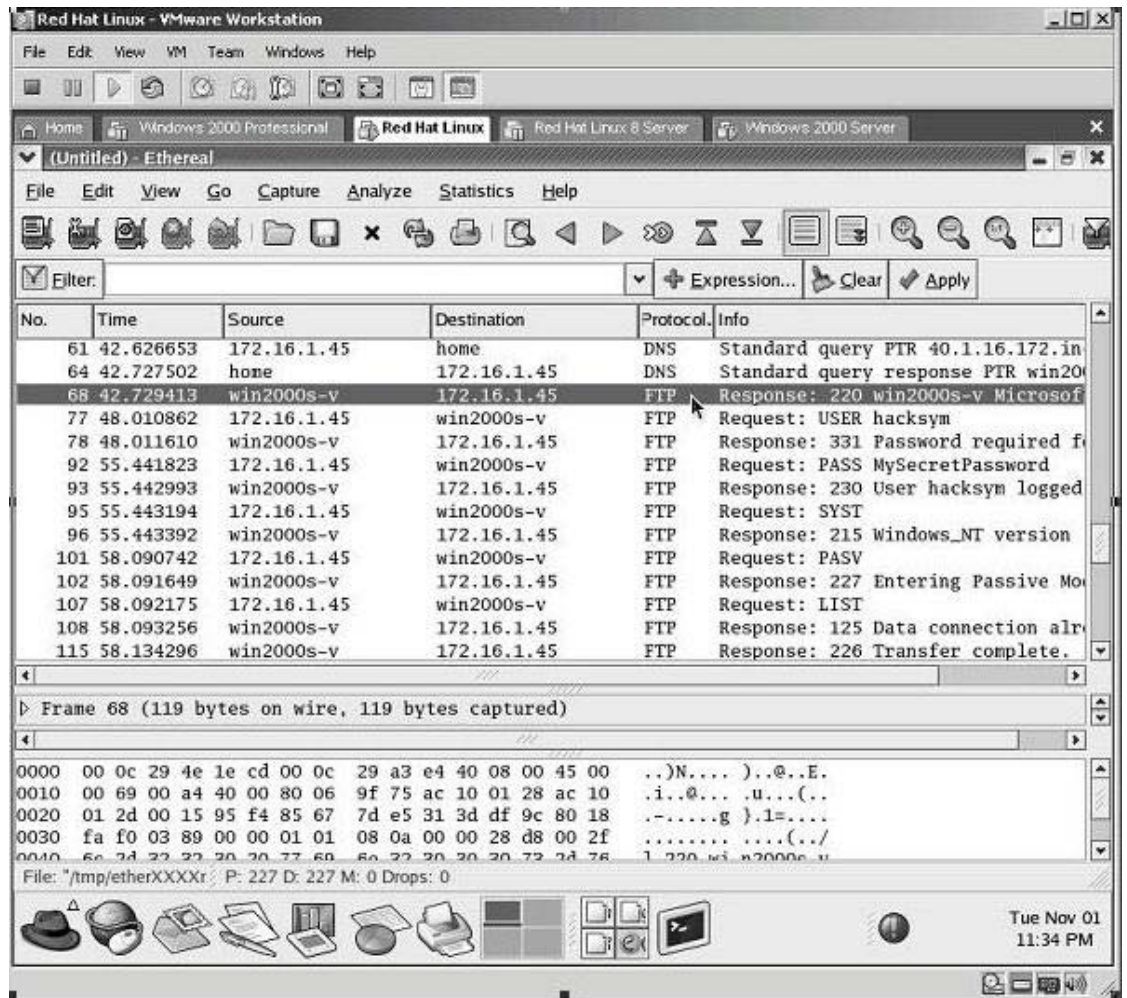
خوب ابتدا بر روی `capture` کلیک کنید بعد به `option` بروید . سپس گزینه `Enable network name resolution` رو تیک بزنید و بعد روی `start` کلیک کنید .



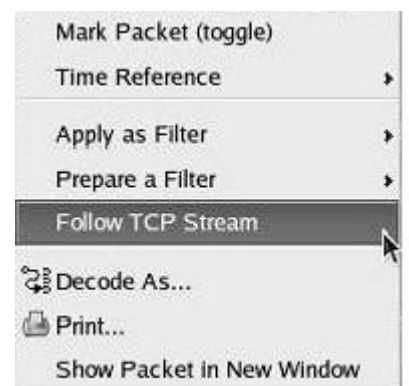
در تصویر زیر همان طور که میبینید تمامی پروتکل ها لیست شده اند و هر مقدار از هر packet که ضبط شده باشد برای شما نمایش داده میشه :



ابتدا به یک ftp متصل میشم و میخوام ببینم که نرم افزار بسته ها رو پیدا میکنه یا نه ؟
من با فرمان **ftp 172.16.1.40** به این پروتکل متصل میشم
و حالا میبینید بسته ها رو پیدا کرده که بر روی شبکه در حال عبور هستن .



البته شما باید پروتکل مورد نظر را انتخاب کنید که ما اینجا قصد داشتیم **ftp** را بررسی کنیم و برای انتخاب پروتکل مورد نظر باید بر روی عبارت **protocol** کلیک کنید مثل تصویر بالا خوب حالا روی یکی از بسته ها کلیک راست کنید و گزینه **Follow TCP Stream** را انتخاب کنید .



خوب حالا چنین چیزی را مشاهده میکنید :

```

Follow TCP stream
Stream Content
220 win2000s-v Microsoft FTP Service (Version 5.0).
USER hacksym
331 Password required for hacksym.
PASS MySecretPassword
230 User hacksym logged in.
SYST
215 Windows_NT version 5.0
PASV
227 Entering Passive Mode (172,16,1,40,4,7).
LIST
125 Data connection already open; Transfer starting.
226 Transfer complete.

```

دقت کردید که **user** و **pass** ها برای نفوذ گر به نمایش در آمدند! به همین راحتی به همین خوشمزگی!!



طریقه ی نصب در ویندوز نیاز به توضیح نداره و خیلی آسونه و وقتی هم که نصب شد ، کار کردن باهاش مثل همون نسخه لینوکسه !

اسنیفر بعدی که خدمتتون معرفی میکنم **ngrep** نام دارد

این اسنیفر **Transfer Control Protocol** یا همون **(tcp)** ، **User Datagram Protocol** یا **(udp)** ،

یا **Internet Control Messenger Protocol** یا **(icmp)** ، **Internet Group Management Protocol** یا

(igmp) و **Serial Line Interface Protocol** (**slip**) را پشتیبانی میکند . با این اسنیفر قدرتمند میتوان اطلاعات

بسیار خوبی از جاسوسی در شبکه بدست آورد . این اسنیفر برای لینوکس و ویندوز نوشته شده . برای استفاده در

لینوکس باید آن را کامپایل کرد که ما در این جا توضیح خواهیم داد !



برای لینوکس

یک دایرکتوری باز کنید و بنویسید `tar -zxvf ngrep-1.40.1.tar.gz` حالا در مرحله بعد در یک دایرکتوری جدید تایپ کنید `cd ngrep` و حالا اینتر بزنید . سپس برای نصب و کامپایل نرم افزار این عبارت را تایپ کنید `./configure` مثل تصویر زیر :



```
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
[root@localhost ngrep]# cd ngrep
[root@localhost ngrep]# ./configure
```

در این تصویر مراحل اولیه کامپایل را مشاهده میکنید :

در این مرحله باید تایپ کنیم : `make`

خوب حالا دوباره یک سری مراحل دیگه طی میشه (بقول معروف یه مشت مزخرف نوشته میشه !!! که البته مزخرف نیست ولی برای مبتدی ها قابل درک نیست)

بعد از این مراحل نرم افزار کامپایل و آماده ی استفاده میشه

در دایرکتوری تایپ میکنیم `./ngrep`. خوب حالا اسنیفر فعال میشه و تمام ترافیک شبکه رو ضبط یا همون

capture میکنه و شما میتونید در دایرکتوری تمام اطلاعات رد و بدل شده رو مشاهده بفرمایید .

برای `stop` کردن عملیات `capture` کلید `ctrl` رو پایین نگه دارین و سپس کلید `C` رو فشار بدین .

خوب به شکل زیر دقت کنید که چطوری اسنیفر تمام اطلاعات شبکه رو برای ما ضبط کرده

```

root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
[root@localhost ngrep]# ./ngrep
interface: eth0 (172.16.0.0/255.255.0.0)
#
T 172.16.1.45:45145 -> 64.233.187.99:80 [AP]
GET / HTTP/1.1..Host: www.google.com..User-Agent: Mozilla/5.0 (X11; U; Linu
x i686; en-US; rv:1.2.1) Gecko/20030225..Accept: text/xml,application/xml,a
pplication/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png
,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1..Accept-Language: en-us, en;
q=0.50..Accept-Encoding: gzip, deflate, compress;q=0.9..Accept-Charset: ISO
-8859-1, utf-8;q=0.66, *;q=0.66..Keep-Alive: 300..Connection: keep-alive..C
ookie: PREF=ID=a63bcbaafd4826388:TM=1130803911:LM=1130803911:S=09Lh7NeNCilIK
UQP....
###
T 64.233.187.99:80 -> 172.16.1.45:45145 [A]
HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-E
ncoding: gzip..Server: GWS/2.1..Content-Length: 1346..Date: Fri, 11 Nov 200
5 22:43:15 GMT.....VYs.6.~.....TK..XI."..I.....9}....%...P.h.q..
..!K>.jF".....E..BDA.4...,%.....=...iG.....pi}.8',.....|>....r+ :U*
....*0..=.F;.J..6..a9... ).....jN..PiF.40.7;..5SB..g..0.[.?.E;.....
....d.+IL..\'..U..<N..q.....^.>..!.C..M6..1.5..WZ.64.=.....h.)f..^.%k;..A
.....`.....A..k.....[.....~x..g..x...l..J..2....=o..VZ...+00..w.
.....8...>K..qu...M&Dp.-l.H...l6..bB.U...J.+.....:2|N...x...y.0L-h,9..
.X..t8!..0%e\f...I...<y8.LvQ..&.w&C.....Q.PA...h.....y.+/.z..a..
....8..7f..y...$.....Yu..97..R...^^.e...R\....=h.$.....N..j..dl....c.

```

اما به چیز دیگه اونم این که ما در این مرحله میخوایم خروجی ها رو در یه فایل txt ذخیره کنیم

برای این منظور تایپ کنید `./ngrep >> output.txt`

دقت کنید که در عبارت بالا output اسم فایل ما هست که میخوایم در اون اطلاعات رو ذخیره کنیم

خوب حالا اطلاعات ذخیره شد ، اما چطوری به اون ها دست پیدا کنیم ؟ با تایپ کردن این فرمان در دایرکتوری میتونید

اطلاعات ذخیره شده رو ببینید : `cat output.txt`

خوب حالا وقتی صفحه بالا بیاد ما میتونیم خروجی ها رو ببینیم ، به این صورت :

```
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
...'.SMBT.....
#
T 172.16.1.40:139 -> 172.16.1.43:1444 [AP]
...'.SMBT.....'....
###
T 172.16.1.45:45145 -> 64.233.187.99:80 [AP]
GET / HTTP/1.1..Host: www.google.com..User-Agent: Mozilla/5.0 (X11; U; Linu
x i686; en-US; rv:1.2.1) Gecko/20030225..Accept: text/xml,application/xml,a
pplication/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png
,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1..Accept-Language: en-us, en;
q=0.50..Accept-Encoding: gzip, deflate, compress;q=0.9..Accept-Charset: ISO
-8859-1, utf-8;q=0.66, *;q=0.66..Keep-Alive: 300..Connection: keep-alive..C
ookie: PREF=ID=a63bcbafd4826388:TM=1130803911:LM=1130803911:S=09Lh7NeNCiIK
UQP....
###
T 64.233.187.99:80 -> 172.16.1.45:45145 [A]
HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-E
ncoding: gzip..Server: GWS/2.1..Content-Length: 1346..Date: Fri, 11 Nov 200
5 22:45:11 GMT.....V.o.0.....+Xuq.....n.XR.vK. ...0....:ID)&.8i..}
G=.;.w.l...x.)w.r{.(...&QP..S.....^...V.Z.....T...0'./.....5.2
.....c....h....jh.f...q-...QJ.....T...fd@.t~.3^\3%.>-6..c...Q.....0.K./
.zZif.....u.XU'..t...0..ZX.....2;d..d.k..\C.z~..+CC.cx.)0...gv...X.....
..jn...JA...?.l.....0.....o=...0.G.P...}.Q[.8U.....5.JKbu...I{...
-S:.W.gu..gi.l.Na.....m..E.....(&.Y.i-...I.RH.*..3..C.....Q.0....4.0
```

در مثال بالا قربانی ما از سایت گوگل بازدید کرده است و تمامی اطلاعات بدست ما رسیده است .



استفاده از نرم افزار ngrep در ویندوز

ابتدا فایل را دانلود کرده و سپس به پوشه مورد نظر بروید (از طریق داس) سپس این فرمان را تایپ کنید :

Ngrep

بعد از زدن اینتر ، نرم افزار شروع به ضبط کردن تمامی اطلاعات سرگردان بر روی شبکه میکند به این صورت :

```

C:\WINNT\System32\cmd.exe - ngrep
C:\Downloads\ngrep\ngrep-1.44>ngrep
NGrep for Windows v1.44 (6/30/05)
Original version (WinPCap is required) : http://ngrep.sourceforge.net
This version (works without WinPCap) : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3 : http://microolap.com/pssdk

interface: \ (172.16.0.0/255.255.0.0)
-

```

و برای stop کردن عملیات capture کلید ctrl را پایین نگه دارید و سپس کلید C را فشار دهید نتیجه ضبط کردن اطلاعات بصورت زیر است :

```

C:\WINNT\System32\cmd.exe
Host: www.google.com..Connection: Keep-Alive..Cookie: PREF=ID=348cf575ffe0828c:TM=1131069917:LM=1131069917:S=7a4dsSx0HU0U3kGd....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [A]
HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-Encoding: gzip..Server: GWS/2.1..Content-Length: 1535..Date: Sat, 12 Nov 2005 01:18:57 GMT.....W.S.6.....$.I.....X.JK...8..m..Hr.e.</7w.l.Hy.W...3n...w$.#...<.Z...s.9.....B..4...Q..0..R...!...L~...-..Tg.?<...T+W.K.X..U..l.u.>...W1...8.....g>...<"i<^i$.^Av..H\...U.3.w.F..C.r...q...W.....q.BM9C*.W...2...a...B+.f..Bf.P.....U..8!...1.@.f...g9..Ua.k'.6...P..U'.v'..7L.....n8I.Z.lg.AB..o.....gg*.~am.dz-..$CZ...D4.8.<..<HJ...!K.$q4B.e.^<.W..d.w..U.....q.y.L..L<.P.zz4I...!F5D..2...#...I...>C.zzn.ll...t..G.nP3..9;a.4F.....P8$.w!l%..o...a.4..9...3q..8..b..9..y..d>k?...%..k..P$.Y5.8.....n...g*.HY...U1...T...~>..9...;Ph.o.h.f.Q...a...s...8G)+.#.i..E...QfNs.Cz<t d>.....6...x.../9..+.*.<.C.Se...7f6..n..G..U...".9.ebz."X.)b8'^.79";.g.G2.A...2...I~..A.a?../.y.8.0..9...#..P>5.....n.....S...ur.9.Y3..W!6...6.m.G..0.....Q...k.)...z..iz.$..L.y.m...p>..w..NP...0.K.yc...fM...S...C.....mj..tJ.=.....'..q.H^.....$/CrPZz...#H...p...<.#<bY!X...;.._d...9.o.EC..Gf/;...8sU..q...&.w..U...I...U..f.Ii.)..R.h...X...KR.I<+...<P>.2X%.N.k...5M.2Qhdf1/.QDXU...%H^T..Z..5.U.9.8")!..j.dR...5..c\S..IV..2..t.*..F..pe2.....n...i#AGEx~y.v...+f'.....l.....1.ItU...*B..z...[z.....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [AP]
3.....Z..f.I.....bw.9...z.>5...&.....#..s%"5U.f..X.D.<..P....9...i...:YQ..l.&Kp...=..e.....<35!.....xNab.Q...#.2...#.0.A...8e_7m15.C...tl...M..&.....W...ZN.\>.....Z%.a...>...;.....Z.....!..?y!...Y5.X.....y...w.8..r.9.MZ~..0.....Qz.?.....
##
T 172.16.1.43:1461 -> 64.233.187.99:80 [AP]
GET /intl/en/images/logo.gif HTTP/1.1..Accept: /*/*..Referer: http://www.google.com/..Accept-Language: en-us..Accept-Encoding: gzip, deflate..If-Modified-Since: Mon, 25 Apr 2005 21:06:18 GMT..User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)..Host: www.google.com..Connection: Keep-Alive..Cookie: PREF=ID=348cf575ffe0828c:TM=1131069917:LM=1131069917:S=7a4dsSx0HU0U3kGd....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [AP]
HTTP/1.1 304 Not Modified..Content-Type: text/html..Server: GWS/2.1..Content-Length: 0..Date: Sat, 12 Nov 2005 01:18:57 GMT....
#exit
74 received, 0 dropped
C:\Downloads\ngrep\ngrep-1.44>

```


اما خواندن و ویرایش اطلاعات در صفحه ی داس کمی مشکل است . برای ذخیره کردن اطلاعات در فایل **txt** از این فرمان استفاده کنید : **ngrep >> output.txt**

که این طوری بعد از **stop** کردن عملیات (البته باید اجازه بدین چند دقیقه ایی اسنیفر فعال باشه تا شبکه رو آنالیز کنه) بعدش در همون فولدری که نرم افزار وجود داشت میتونید فایل رو ببینید که ذخیره شده و بعد از باز کردن اون میتونید اطلاعات رو ببینید . که برای من اطلاعات به این صورت در اومده :

```

output - WordPad
File Edit View Insert Format Help
U 172.16.1.43:1468 -> 172.16.0.1:53
.h.....ftp.hackme.net.....
#
U 172.16.0.1:53 -> 172.16.1.43:1468
.h.....ftp.hackme.net.....@.....V.....ns2.....
V.....ns1..
###
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
220 Serv-U FTP Server v5.0 for WinSock ready.....
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
USER hacker..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
331 User name okay, need password...
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
█PASS hacktheplanet..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
230 User logged in, proceed...
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
QUIT..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
221 Goodbye!..
####exit
65 received, 0 dropped
For Help, press F1

```

در مثال بالا این اطلاعات بدست اومده :

- Username
- Passwords
- E-mails
- IP addresses
- Media Access Control (MAC) addresses
- Router IP addresses



اسنیفر بعدی که خدمتون معرفی میکنیم

نرم افزار مشهور tcpdump میباشد

این اسنیفر برای لینوکس نوشته شده . اما ما در این قسمت طریقه ی نصب را بصورت تشریحی بیان میکنیم و از درج تصاویر بصورت مرحله به مرحله معذوریم .

ابتدا در دایرکتوری تایپ کنید : `tar -zxvf tcpdump-3.9.3.tar.gz.`

وقتی عملیات به اتمام رسید در یک دایرکتوری جدید این عبارت را تایپ کنید : `tcpdump-3.9.4.`

خوب حالا باید دایرکتوری رو عوض کنیم با این فرمان : `cd tcpdump-3.9.4`

حالا نرم افزار برای کامپایل آماده میشه و ما باید تایپ کنیم : `./configure`

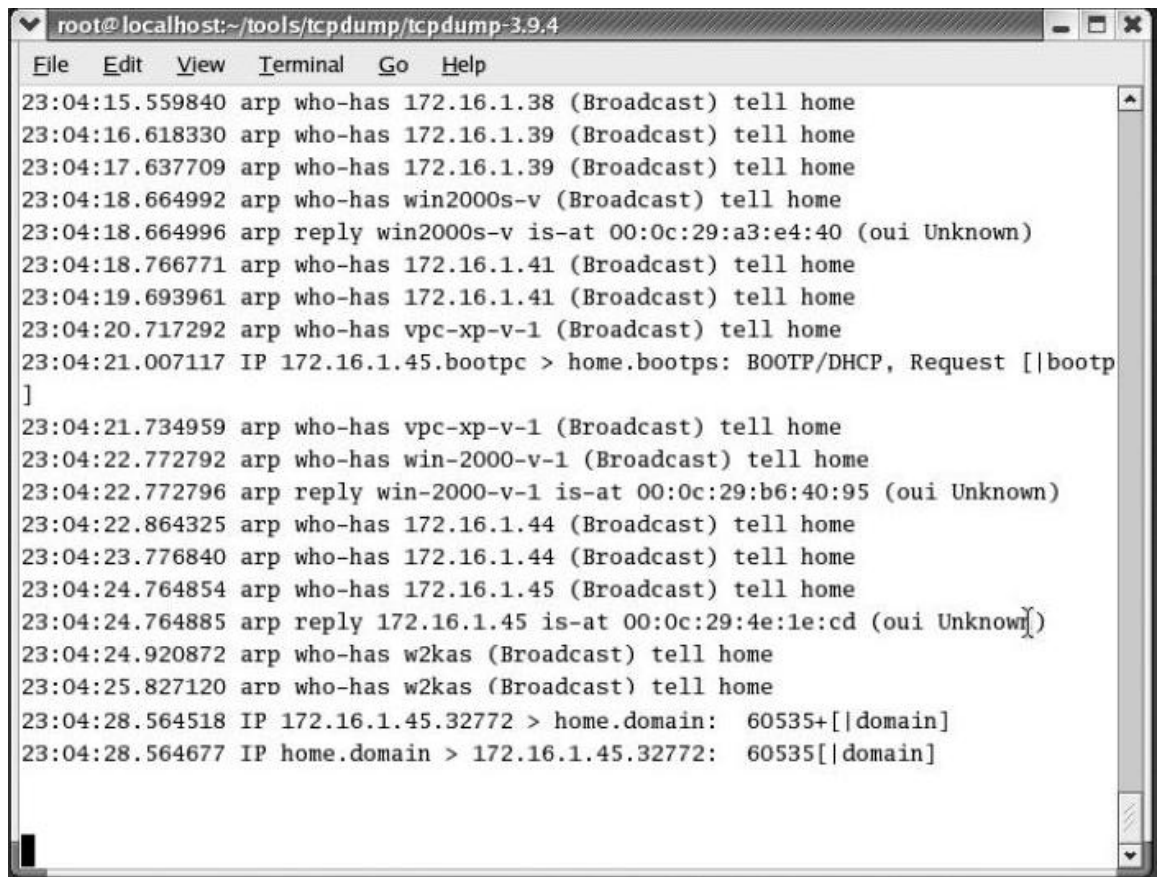
بعد از این کار یک سری نوشته میاد و میره و شما باید بعد از اتمام این نوشته ها تایپ کنید : `make`

و بعدش هم اینتر بزنید ، باز میاد و میره ، حالا شما باید تایپ کنید `make install`

و سپس اینتر بزنید . بعد از این که نوشته ها اومد و رفت نرم افزار با موفقیت کامپایل میشه . حالا شما میتونید با تایپ

این دستور در کامند اسنیفر رو فعال کنید : `./tcpdump`

من با تایپ این فرمان چنین چیزی رو مشاهده کردم :



```
File Edit View Terminal Go Help
23:04:15.559840 arp who-has 172.16.1.38 (Broadcast) tell home
23:04:16.618330 arp who-has 172.16.1.39 (Broadcast) tell home
23:04:17.637709 arp who-has 172.16.1.39 (Broadcast) tell home
23:04:18.664992 arp who-has win2000s-v (Broadcast) tell home
23:04:18.664996 arp reply win2000s-v is-at 00:0c:29:a3:e4:40 (oui Unknown)
23:04:18.766771 arp who-has 172.16.1.41 (Broadcast) tell home
23:04:19.693961 arp who-has 172.16.1.41 (Broadcast) tell home
23:04:20.717292 arp who-has vpc-xp-v-1 (Broadcast) tell home
23:04:21.007117 IP 172.16.1.45.bootpc > home.bootps: BOOTP/DHCP, Request [|bootp
]
23:04:21.734959 arp who-has vpc-xp-v-1 (Broadcast) tell home
23:04:22.772792 arp who-has win-2000-v-1 (Broadcast) tell home
23:04:22.772796 arp reply win-2000-v-1 is-at 00:0c:29:b6:40:95 (oui Unknown)
23:04:22.864325 arp who-has 172.16.1.44 (Broadcast) tell home
23:04:23.776840 arp who-has 172.16.1.44 (Broadcast) tell home
23:04:24.764854 arp who-has 172.16.1.45 (Broadcast) tell home
23:04:24.764885 arp reply 172.16.1.45 is-at 00:0c:29:4e:1e:cd (oui Unknown)
23:04:24.920872 arp who-has w2kas (Broadcast) tell home
23:04:25.827120 arp who-has w2kas (Broadcast) tell home
23:04:28.564518 IP 172.16.1.45.32772 > home.domain: 60535+[|domain]
23:04:28.564677 IP home.domain > 172.16.1.45.32772: 60535[|domain]
```

خوب از اونجایی که این اسنیفر خیلی کاربرد داره چند تا دستور مشهور دیگه رو هم بررسی میکنیم

برای متمرکز شدن روی یک سایت یا آی پی خاص از این فرمان استفاده میکنیم :

tcpdump host (Target IP or Hostname)

یکی از دلایلی که این اسنیفر خیلی مشهوره همین قابلیت بالاییه !

برای مشاهده اطلاعاتی که فقط به یک قربانی مربوط میشه از فرمان زیر استفاده میکنیم :

tcpdump dst host (Target IP or Hostname)

برای اسنیف کردن یک پروتکل مخصوص مثلا tcp یا udp میتونید از این فرمان استفاده کنید :

tcpdump dst host (Target IP or Hostname) && (tcp dst port 80 or tcp dst port 443)



کار با اسنیفر windump

خوب این اسنیفر برای ویندوز نوشته شده و در واقع همون اسنیفر بالاییه که این نسخه از اون در ویندوز کارایی داره . با این نرم افزار باید در محیط خط فرمان یا همون داس کار کنید . اطلاعات ضبط شده توسط اسنیفر میتونه save بشه . این نرم افزار در ویندوز های 98 به بالا کارایی دارد . دوستان دقت کنید که برای استفاده از این نرم افزار حتما باید winpcap رو نصب کنید .

با این نرم افزار میشه تمام شبکه رو با قدرت بسیار زیاد مورد جاسوسی قرار داد . شما برای تمرین میتونید در یک شبکه ، که تمام رایانه های اون به یک هاب وصل شدن ، این نرم افزار رو فعال کنید . سپس تمام اطلاعات کسانی که به شبکه دسترسی دارند برای شما به نمایش در میاد و شما میتونید قدرت نرم افزار رو ببینید .

برای فعال کردن اون ، در کامند تایپ کنید : windump >> output.txt

حتما میدونید که output.txt برای ذخیره کردن اطلاعات در اون هست . چون وقتی اطلاعات در کامند به نمایش در بیاد خوندن و ویرایش اون ها سخت میشه . بعد از این که اینتر زدید چنین چیزی رو مشاهده خواهید کرد :
برای stop کردن عملیات ضبط بسته ها ابتدا کلید Ctrl رو پایین نگه دارین و سپس کلید C رو فشار بدین . بعد همون فایل متنی رو باز کنید و اطلاعات رو ببینید . مثل تصویر زیر

```

output - Notepad
File Edit Format Help
11:44:05.923774 IP 64.233.187.99.80 > win-2000-v-1.1420: P 13732:14003(271) ack 3388 win 8576
11:44:05.923817 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 14003 win 64240 (DF)
11:44:05.928344 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1156:1541(385) ack 382 win 63859 (DF)
11:44:05.977672 IP 64.233.187.99.80 > win-2000-v-1.1421: P 382:509(127) ack 1541 win 8576
11:44:06.111710 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3388:3667(279) ack 14003 win 64240 (DF)
11:44:06.165217 IP win-2000-v-1.1421 > 64.233.187.99.80: . ack 509 win 63732 (DF)
11:44:06.165388 IP 64.233.187.99.80 > win-2000-v-1.1420: . 14003:15433(1430) ack 3667 win 8576
11:44:06.165426 IP 64.233.187.99.80 > win-2000-v-1.1420: P 15433:15705(272) ack 3667 win 8576
11:44:06.165671 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 15705 win 64240 (DF)
11:44:06.175204 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1541:1926(385) ack 509 win 63732 (DF)
11:44:06.207416 IP 64.233.187.99.80 > win-2000-v-1.1421: P 509:636(127) ack 1926 win 8576
11:44:06.249917 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3667:3946(279) ack 15705 win 64240 (DF)
11:44:06.303519 IP 64.233.187.99.80 > win-2000-v-1.1420: . 15705:17135(1430) ack 3946 win 8576
11:44:06.304359 IP 64.233.187.99.80 > win-2000-v-1.1420: P 17135:17409(274) ack 3946 win 8576
11:44:06.304404 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 17409 win 64240 (DF)
11:44:06.320485 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1926:2311(385) ack 636 win 63605 (DF)
11:44:06.397590 IP 64.233.187.99.80 > win-2000-v-1.1421: P 636:763(127) ack 2311 win 8576
11:44:06.493387 arp who-has ppp-70-254-207-50.dsl.hstntx.swbell.net (Broadcast) tell home
11:44:06.498135 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3946:4225(279) ack 17409 win 64240 (DF)
11:44:06.553310 IP 64.233.187.99.80 > win-2000-v-1.1420: . 17409:18839(1430) ack 4225 win 8576
11:44:06.553962 IP 64.233.187.99.80 > win-2000-v-1.1420: P 18839:19111(272) ack 4225 win 8576
11:44:06.554002 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 19111 win 64240 (DF)
11:44:06.561519 IP win-2000-v-1.1421 > 64.233.187.99.80: P 2311:2696(385) ack 763 win 63478 (DF)
11:44:06.594907 IP 64.233.187.99.80 > win-2000-v-1.1421: P 763:890(127) ack 2696 win 8576
11:44:06.657523 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4225:4504(279) ack 19111 win 64240 (DF)
11:44:06.704469 IP 64.233.187.99.80 > win-2000-v-1.1420: . 19111:20541(1430) ack 4504 win 8576
11:44:06.707465 IP 64.233.187.99.80 > win-2000-v-1.1420: P 20541:20814(273) ack 4504 win 8576
11:44:06.707544 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 20814 win 64240 (DF)
11:44:06.711358 IP win-2000-v-1.1421 > 64.233.187.99.80: P 2696:3081(385) ack 890 win 63351 (DF)
11:44:06.758053 IP 64.233.187.99.80 > win-2000-v-1.1421: P 890:1017(127) ack 3081 win 8576
11:44:06.847778 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4504:4783(279) ack 20814 win 64240 (DF)
11:44:06.900949 IP 64.233.187.99.80 > win-2000-v-1.1420: . 20814:22244(1430) ack 4783 win 8576
11:44:06.901790 IP 64.233.187.99.80 > win-2000-v-1.1420: P 22244:22517(273) ack 4783 win 8576
11:44:06.901847 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 22517 win 64240 (DF)
11:44:06.906381 IP win-2000-v-1.1421 > 64.233.187.99.80: P 3081:3466(385) ack 1017 win 63224 (DF)
11:44:06.946395 IP 64.233.187.99.80 > win-2000-v-1.1421: P 1017:1144(127) ack 3466 win 8576
11:44:07.004446 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4783:5062(279) ack 22517 win 64240 (DF)
11:44:07.085813 arp who-has 172.16.1.44 tell win-2000-v-1
11:44:07.127807 IP 64.233.187.99.80 > win-2000-v-1.1420: . 22517:23947(1430) ack 5062 win 8576

```

در مثال بالا این اطلاعات مشاهده میشود :

- _ Usernames
- _ Passwords
- _ E-mails
- _ IP addresses
- _ MAC addresses
- _ Router IP addresses

Sniffing with snort !!

بله ! اسنورت هم یک اسنیفر بسیار قدرتمند است . این اسنیفر هم توانایی ضبط اطلاعات روی شبکه را دارا میباشد . شما میتوانید آن را از آدرس www.snort.org دریافت کنید . بعد از نصب نرم افزار در

کامند این دستور را تایپ کنید : `snort -w`

که بعد از این کار چنین جوابی را دریافت میکنیم :

```
C:\Snort\bin>snort -W
```

```
--*> !Snort <*-
```

```
(Version 2.0.0-ODBC-MySQL-WIN32 (Build 72
```

```
(By Martin Roesch (roesch@sourcefire.com, www.snort.org
```

```
[...]
```

```
Interface Device Description
```

```
-----  
1 / Device\NPF_{BB1D0098-0395-4238-B72C-8FB099DDF50C} (UNKNOWN..
```

خوب اگه این نرم افزار کار نکرد علتش اینه که شما winpcap رو نصب نکردین . و میتونید با نصبش این مشکل رو بر طرف کنید .

حالا وقتش رسیده یه تست بکنیم و ببینیم که اسنورت چطوری کار میکنه و توانایی اون چقدره ؟

ابتدا به یک آی پی پینگ میکنیم و از سوئیچ t- هم استفاده میکنیم به این صورت :

```
C:\>ping 10.0.0.1 -t
```

خوب حالا در یک صفحه ی داس جدید دیگه برای فعال کردن اسنورت تایپ کنید :

```
C:\Snort\bin>snort -i 1 -v
```

اگر کارها رو درست انجام داده باشید میتونید این عبارات رو مشاهده کنید که در اون یک بسته از

پروتکل icmp نشون داده شده . که البته فقط این یک بسته ارسال شده بود !

```
C:\Snort\bin>snort -i 1 -v icmp
```

```
Running in packet dump mode
```

```
[...]
```

```
==== Initialization Complete ====
```

```
--*> !Snort <*-
```

```
(Version 2.0.0-ODBC-MySQL-WIN32 (Build 72
```

```
(By Martin Roesch (roesch@sourcefire.com, www.snort.org
```

```
[...]
```

```
192.168.100.1 <- 192.168.100.4 22:13:19.156585-21/04
```

```
ICMP TTL:128 TOS:0x0 ID:16436 IpLen:20 DgmLen:60
```

```
Type:8 Code:0 ID:512 Seq:4864 ECHO
```

```
+++++
```

192.168.100.4 <- 192.168.100.1 22:13:19.157192-21/04

ICMP TTL:255 TOS:0x0 ID:865 IpLen:20 DgmLen:60

Type:0 Code:0 ID:512 Seq:4864 ECHO REPLY

=====
=====

خوب حالا با فرمان **ctrl-c** اسنورت رو غیر فعال کنید و همه ی پنجره های قبلی رو ببندین

این دفعه با اسنورت میخوایم ببینیم که یک **DNS lookup** چطوری انجام میگیره ؟ (چه بسته هایی ارسال میشه؟)

البته در این جا فقط روی پروتکل **udp** تمرکز میکنیم . البته ممکنه نرم افزار **NetBIOS** رو برای ما نشون بده ،

چون جز این پروتکل هست ما میتونیم با تمرکز روی یک پورت خاص ، از این اتفاق جلوگیری کنیم در این مثال ما

روی پورت **53** تمرکز میکنیم . به این صورت :

```
C:\Snort\bin>snort -i 1 -v -X udp and port 53
```

برای یک **DNS lookup** در خط فرمان هم این عبارت رو تایپ میکنیم (دقت کنید که این فرمان ها در صفحه ایی

جداگانه تایپ شوند)

```
C:\>nslookup www.google.com
```

به این ترتیب ما دو بسته رو ارسال میکنیم . ما با استفاده از این اختیارات میتونیم ببینیم که برنامه های کاربردی در

ویندوز دقیقا چیکار میکنن . خوب این که بعدش چه اتفاقی میفته میذارم بر عهده ی خودتون (چون خودتون

میرید دنبالش و یاد میگیرید)

البته ما میتونیم پروتکل های دیگه رو فیلتر کنیم که در زیر من این فرمان ها رو نوشتم :

```
C:\Snort\bin>snort -v icmp or (udp and port 53) or (tcp and (port 25 or 53))
```

خوب حالا من میخوام یه اسنیفر تجاری رو معرفی کنم .

این اسنیفر رو از آدرس زیر دانلود کنید :

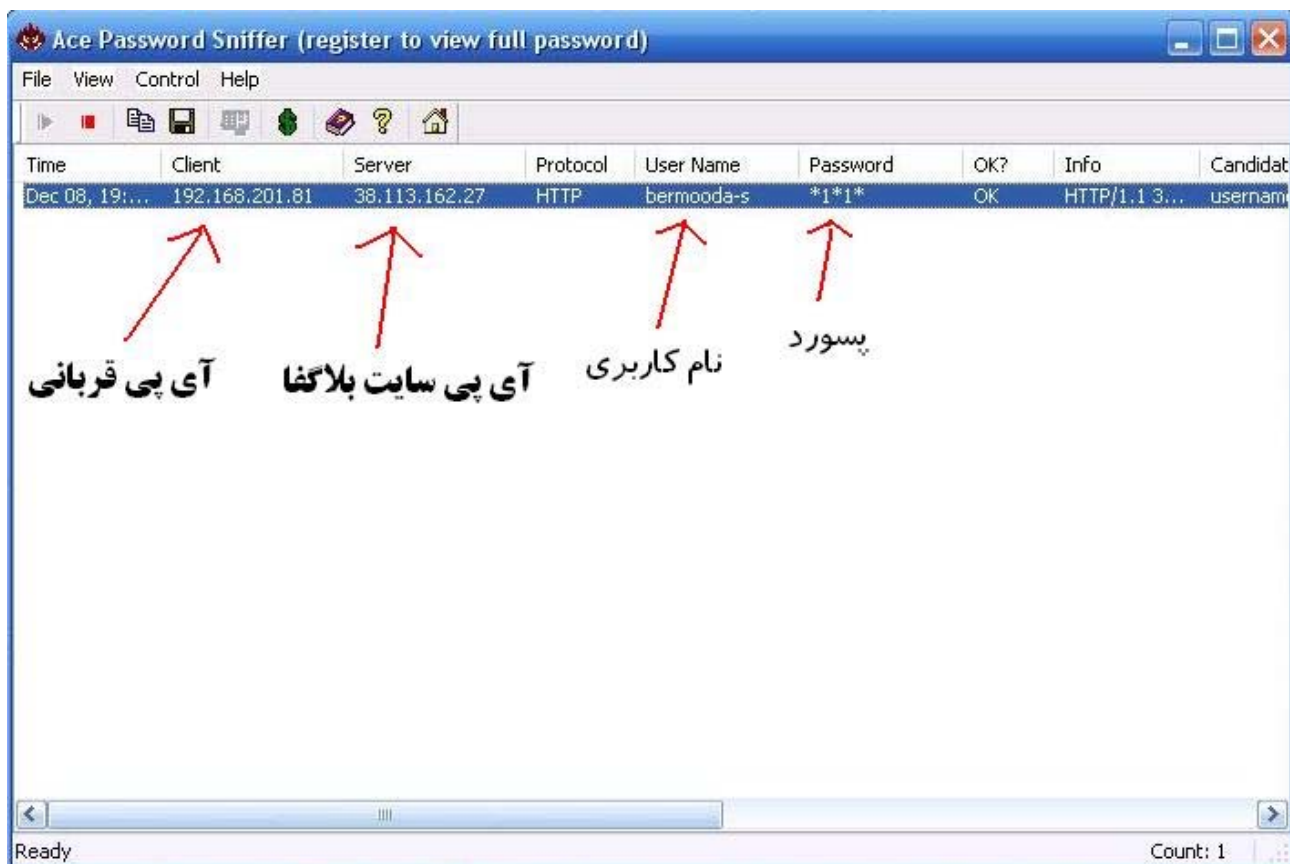
<http://www.efeotech.com/download/ApsSetup.exe>

کار کردن خیلی باهش آسونه و شما فقط باید روی استارت کلیک کنید . بعدش هم طبق معمول کار با اسنیفر ها شما

باید صبر کنید تا یه نفر به یه جایی لاگین کنه و شما پسوردشو بدست بیارید . این نرم افزار قدرت خیلی خوبی داره اما

اگه **register** نکرده باشین کلیه ی اطلاعات رو بصورت یکی درمیون نشون میده مثل این تصویر که پسورد یه وبلاگ

هک شده : (پسورد وبلاگ 11111 است)

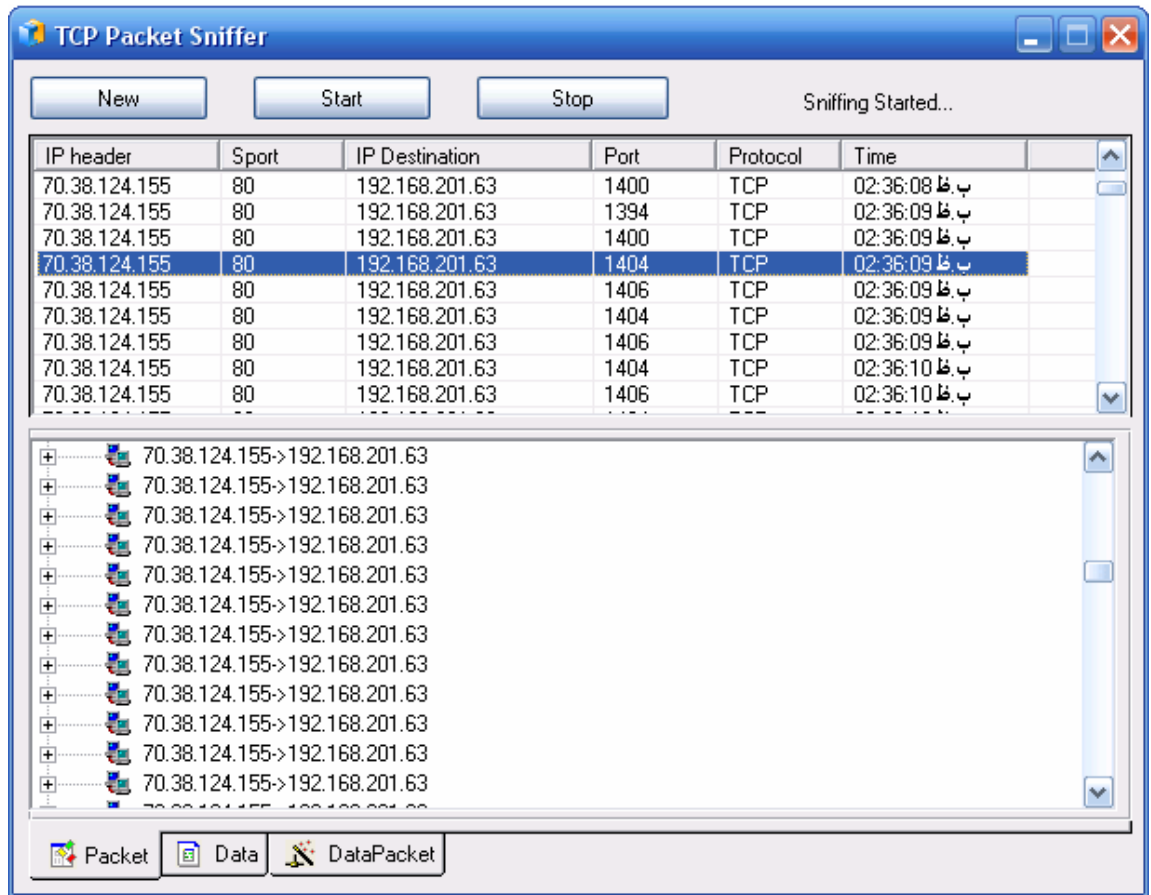


خوب به اسنیفر دیگه هم که برای مدیران شبکه ها میتونه کاربرد داشته باشه رو هم معرفی میکنم

tcp packet sniffer

این اسنیفر در نرم افزار net tools وجود داره و شما میتونید بیشتر بسته های رد و بدل شده رو بررسی کنید

اینم تصویرش :



و اما راه های مقابله با اسنیفر ها

اولین راه (که البته بیشتر راه های مقابله با اسنیفرها هم زیر مجموعه ی همین روش هستند)

یکی از راه های مقابله با اسنیفر hash کردن اطلاعات هست . برنامه های مختلفی وجود دارند که توسط آن ها میتوان این اطلاعات را hash کرد . اما فرض کنید یک هکر بر روی سیستم شما نت کت را آپلود کرده باشد . در این لحظات اگر با اسنیفر بتوانید اطلاعات در حال عبور را ببینید که چه بهتر اما اگر نتوانستید چه کار میکنید ؟ منظورم این است اگر هکر از نرم افزار cryptcat به جای نت کت استفاده کند . اطلاعات hash میشوند . و شما باید مثل خود هکرها این اطلاعات را کرک کنید که ممکن است دقایقی بطول بیانجامد و در طول این مدت هکر تمامی کارهای خود را انجام میدهد و دیگر هیچ که هیچ !!!!

خوب پس دیدید که رمز نگاری کردن اطلاعات مفید ترین و سریع ترین راه مقابله با اسنیفر در شبکه است . حتی بعضی از هکرها اسنیفر را بر روی سرور آپلود میکنند و سپس با خواندن اطلاعات بدون دردسر به خیلی از پسورد های

مهم دست پیدا میکنند . حالا فکرش را بکنید اگر اطلاعات hash شده باشند ! در این لحظه قیافه ی هکر بسیار دیدنی میشود ! چون با این همه زحمت که کشیده بود ، شما همه را بر باد دادید . و این بار به جای هکرها شما یعنی مدیر سرور پیروز میدان خواهید بود !

دومین راه

اما راه بعدی برای جلوگیری از اسنیفرها استفاده از سوئیچ در شبکه های ethernet است . سوئیچ یک ابزار مخصوص شبکه است که بسته ها را تنها به رایانه های مقصد آنها میفرستد. با این وجود با برنامه ریزی سوئیچ برای ایجاد یک پورت انعکاسی یا یک پورت نظارت، و یا با حمله به سوئیچ برای به هم ریختن جداول داخلی آن که مربوط به رایانه ها و آدرسهای شبکههای میشود، امکان نظارت بر ترافیک شبکه های سوئیچ نیز وجود دارد هرچند شبکه های token ring ذاتاً شبکه های عامگستر نیستند، اما در عمل تمام بسته های انتقالی در آنها بطور متوسط از نیمی از واسط های روی شبکه عبور می کنند و لذا نگرانیهای مشابهی در آنها نیز وجود دارد. خلاصهً مطلب اینکه در بیشتر فناوریهای شبکه، جلوگیری و یا حتی شناسایی استراق سمع ممکن نیست و تنها باید فرض را بر آن گذاشت که ترافیک شبکه مورد استراق سمع قرار دارد و سعی کرد با استفاده از رمز گذاری، آنرا برای مهاجم غیر قابل استفاده نمود. البته باید در نظر داشت که حتی در صورت استفاده از رمز گذاری نیز آدرسها و پورتهای مبدأ و مقصد توسط مهاجم قابل کشف و استفاده برای تحلیل ترافیک هستند.

رمز گذاری به طرق مختلفی میتواند به افزایش امنیت ip کمک کند :

رمز گذاری در سطح ارتباط

با رمز گذاری در سطح ارتباط، بسته ها در صورت انتقال روی یک ارتباط دادهای ناامن بطور خودکار رمز گذاری و پس دریافت رمز گشایی میشوند. با اینکار استراق سمع شکست میخورد، چون مهاجم نمیداند چگونه باید بسته ها را رمز گشایی کند. رمز گذاری در سطح ارتباط در بسیاری از محصولات شبکه های رادیویی وجود دارد، اما در سایر فناوریهای عام گستر شبکه مثل ethernet و fddi کمتر یافت میشود. برای مودمها و ارتباطات خطوط مستقیم استیجاری، رمز گذارهای اختصاصی ارتباط نیز بوجود آمده اند.

رمز گذاری در دو انتها

در این روش میزبان فرستنده، محتوای بست ها را رمز گذاری میکند و هنگام دریافت بسته ها در طرف دیگر، این

محتویات بطور خودکار رمزگشایی می شوند. سازمانهایی که در بیش از یک موقعیت فیزیکی قرار دارند برای اتصال به اینترنت از مسیریابهای رمزگذار بهره می گیرند. این مسیریابها بطور خودکار بسته هایی که از یک اداره شرکت به اداره دیگری فرستاده می شوند را بمنظور جلوگیری از استراق سمع مهاجمان اینترنتی رمزنگاری میکنند (این روش تحت عنوان vpn شناخته میشود) اما در عین حال بسته هایی که از سازمان به پایگاه های دیگر فرستاده میشوند را رمزگذاری نمی نمایند .

امروزه این نوع رمزگذاری در سطح بسته بطور عام با استفاده از پروتکل ipsec انجام میگردد (که در RFC شماره 2401 توضیح داده شده است) . ipsec را میتوان برای رمزگذاری غیرمحسوس تمامی ارتباطات میان دو میزبان، ارتباطات میان یک میزبان و یک شبکه، و یا ارتباطات میان دو شبکه بکار برد . استفاده از ipsec روش قدرتمندی برای رمزگذاری خودکار سیستمهایی است که قابلیت رمزگذاری ندارند .

رمزگذاری در سطح برنامه

بجای اتکا بر سخت افزارها برای رمزگذاری، می توان رمزگذاری را در سطح برنامه ها انجام داد . بعنوان مثال نسخه Kerberos از دستور telnet قادر است بطور خودکار محتویات جریانهای داده telnet را در هر دو جهت رمزنگاری کند . پروتکل پوسته امن (ssh) نیز بطور خودکار رمزگذاری جریان داده ها را انجام می دهد . رمزگذاری در سطح برنامه همچنین می تواند از طریق ایجاد تونل یا استفاده از یک پروتکل ثانویه روی یک پروتکل سطح برنامه که در حال کار است انجام گیرد . بعنوان مثال پروتکل پوسته امن این امکان را بوجود میآورد که پورتها و اتصالات tcp/ip بتوانند از طریق یک تونل رمزنگار از یک میزبان به میزبان دیگر منتقل شوند . با استفاده از پروتکل های ssl و tls روی سرویس دهنده ها و سرویس گیرنده های منفرد برنامه ای، آنها را نیز میتوان به همین صورت ایمن نمود . استفاده صرف از رمزنگاری کافی نیست، بلکه برای ایجاد حفاظت، رمزگذاری باید بصورت صحیح پیاده سازی شود . همانطور که در بالا بحث شد، استاندارد اصلی رمزگذاری برای شبکه های محلی بیسیم مبتنی بر پروتکل 802.11b (WEP) به هیچ وجه محرمانگی واقعی را ایجاد نمیکند؛ چرا که پیاده سازی آن دچار نقص است و یافتن کلید رمزگذاری مورد استفاده در سیستمهای wep کار چندان مشکلی نیست .

خوب دوستان مقاله به پایان رسید در آخر مقاله هم چند تا عکس قرار میدم که امیدوارم خوشتون بیاد :

اولین عکس آکادمی هکرها :



اینم 10 هکر برتر سال 2003 : (قیافه هاشون خیلی خلاصه البته به جز کوین متینک که

قیافش غلط اندازه ☺)



ایشون هم استاد مخ زنی در زمینه هک ، جناب کوین متنیک :



این کیه ؟ نمیدونم ! 😊



اینم دکتر mudge :



منابع این کتاب :

1) **Practical Hacking Techniques And Countermeasures**

2) **IT Security Handbook** (راهنمای امنیت فناوری اطلاعات)

3) اطلاعات و تجربیات شخصی !!!

معرفی کتاب

(البته شاید این کتاب کمی قدیمی باشه ولی درباره ی مباحث **tcp/ip** مطالب خوبی رو گفته که مطمئن هستم برای

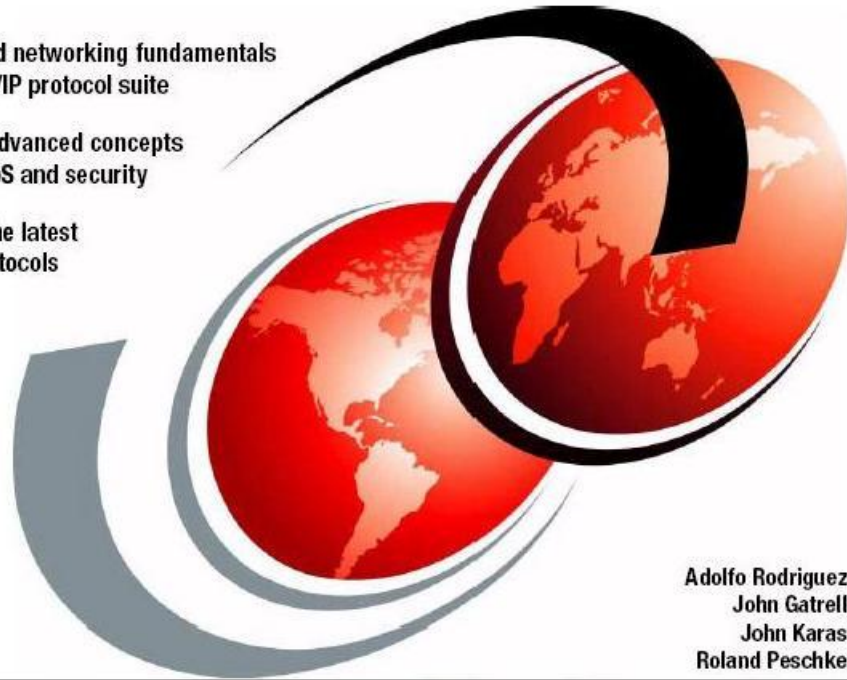
همه میتونه مفید باشه) :

TCP/IP Tutorial and Technical Overview

Understand networking fundamentals of the TCP/IP protocol suite

Contains advanced concepts such as QoS and security

Includes the latest TCP/IP protocols



Adolfo Rodriguez
John Gatrell
John Karas
Roland Peschke

