زکات علم آموزش و انتقال آن به دیگران است

مجموعه مقالات ایمن سازی ویندوز

پیدا کردن پورت های باز روی ویندوز و مسدود کردن آنها

نویسنده : **مسلم حقیقیان**

دانشجوی رشته کامپیوتر- نرم افزار، دانشگاه یزدان پناه سنندج

FINDING OPEN PORT ON THE WINDOWS AND BLOCK THEM

KURD BLACK HAT SECURITY TEAM

AUTHOR : MOSLEM HAGHIGHIAN

EMAIL:

L4TR0D3CTISM@YAHOO.COM

L4TR0D3CTISM@GMAIL.COM

Greeting to

WWW.GREYH4T.COM

WWW.BLACK-HG.ORG

We Are :

Net.Edit0r, A.Cr0x, 3H34N, l4tr0d3ctism ,4ut0n0m0us, G3n3Rall, IrIsT, NoL1m1t, Mohammad_Reza

My Freand in other Team :

Kurd.Blackhat , R3bin.kurd , Dr Toofan , Niaamarek , dj TiniVini , Bl4ck.Viper , Ashi Bomba

سخنی با خوانندگان

فقدان معنویت و بی بند و باری اخلاقی در عرصه ی های مختلف جلوه هایی زشت و مخرب را به نمایش می گذارد و ما ظهور این پدیده را بین برخی از هکر ها و برنامه نویسان کامپیوتری در قالب ایجاد ویروس و بد افزار های کامپیوتری جهت ایجاد اختلال و تخریب و دزدی در در سیستم عامل ها به صورت معضلی جدی شاهد هستیم و لذا ضرورت ایجاد امنیت و طراحی دیوار های دفاعی در قالب آنتی ویروس و فایروال ها شرکت های امنیتی را به تکاپو و پیشرفت واداشت و پر واضع است که مقابله و واکنش متناسب در مقابل سرقت و تجاوز به حریم خصوصی دیگران کاری پر اهمیت و ارزشمند تلقی می گردد و در این راستا مسائل مختلفی مطرح و مد نظر قرار گرفت ، یکی از موارد قابل توجه قابلیت ها و محدوده ی تاثیر گذاری بد افزار بر روی سیستم عامل زیرا فایروال ها و آنتی ویروس ها می توانند از ورود ویروس به سیستم جلوگیری نمایند و یا در صورت وجود ویروس آن را حذف نمایند ولی آثار تخریبی ایجاد شده را به طور کامل نمی توانند از بین ببرند .یکی از عملیات منفی بد افزار ها و مخصوصا جاسوس افزار ها باز کردن یک پورت جهت نفوذ به سیستم عامل و یا تبادل اطلاعات می باشد که ضد ویروس به صورت اتوماتیک نمی تواند آن را مسدود نماید .

در این نوشتار مقدماتی شما با نحوه ی شناسایی پورت و شوه ه مسدود کردن آنها آشنا می شوید . این حقیر می خواهم در ایجاد امنیت و جلوگیری از بی بند و باری در این عرصه و مقابله با بی اخلاقی و سرقت و حفاظت از حریم شخصی افراد سخم کوچکی داشته باشم وامیدوارم با این مقاله در آشنا کردن خوانندگانی با مقولات فوق الذکر آنایی ندارند قدمی برداشته باشم و لذا از اساتیر محترمی که این نوشته را میخوانند به لحاظ کمی بضاعت علمی و مقدماتی بودن آن پوزش می خواهم و خود را همواره محتاج راهنمایی آنها می دانم .

فهرست :

تعريف پورت

متداولترين پورت ها

پويش پورت ها و خطر باز بودن پورت بر روي سيستم شما

پيدا كردن پورت هاي باز بر روي سيستم عامل

- فرمان Netstat
- با استفاده از نرم افزار X-netstat
- نرم افزار Cureport
- برنامه Port Manager
- با استفاده از Scanner ها
  - Online port Scanner
  - ابزار Local Port Scanner
  - FreePortScanner

بستن پورت ها بر روي ويندوز

- با استفاده از بستن سرويس ها
  - با استفاده از كنسول Services.msc
  - با استفاده از System Configuration Utility
  - Net Command
  - فرمان SC
  - متوقف كردن سرويس ها در رجيستري جهت مسدود شدن پورت آنها
  - استفاده از ابزار Turbo Service Manager
  - با استفاده از ابزار Service Studio

- كار با پورت ها با استفاده از فايروال ويندوز
  - با استفاده از برنامه Windows Firewal
  - بستن پورت ها با استفاده از فرمان Netsh

- مسدود كردن پورت ها از طريق فايروال هاي معروف
  - Nod32 Smart Security
  - بستن پورت با استفاده از فايروال Comodo
  - بستن پورت با Kaspersky internet security
  - بستن پورت با استفاده از Norton internet Security

- بستن پورت از طريق كد هاي VBS

تعریف پورت

پورت در لغت نامه به معناي بندرگاه آمده . كلا به درگاه ورودي خروجي هر سامانه ميتوان واژه پورت را اطلاق كرد .

شما در قطعات سخت افزاري و هم در نرم افزاري نياز به درگاه ورودي و خروجي تعريف شده اي داريد كه ان درگاه كه تمامی ورودی ها و خروجی ها از طریق این درگاه ها صورت می گیرد .

در رايانه با دو نوع پورت سر و كار داريم . پورت هاي سخت افزاري و پورت هاي نرم افزاري .

پورت هاي سخت افزاري چند نوع است كه عمدتا سريالي و موازي هستند كه كه در اين درس ما با آن سرو كار نداريم

بحث ما فعلا نرم افزاري و مربوط به وب است و حتما شما واژه پورت را زياد شنيده باشيد.

در نرم افزاري به خلاف سخت افزاري تعداد پورت ها خيلي بيشتر از آن است . به يكباره تعداد دوبايت را براي آن در نظر گرفته اند !! و اين رقم بزرگي بنظر مياید و تا جاييكه به پورت هاي مصرف شده نگاه ميكنيم ميبينيم چندان پر نشده اند و شما كلا ميتوانيد براحتي براي نرم افزار هايي كه برنامه نويسي ميكنيد يک پورت خاص را برای برنامه ی خودتان که در شبکه در حال تبادل اطلاعات است را باز كنيد .

مدل TCP/IP از پروتکل های مختلفی استفاده می کند که اساسی ترین آنها TCP و UDP می باشند . هر یک از این پروتکل ها می توانند دارای ۶۵۵۳۵ پورت باز داشته باشند . سیستم عامل بر اساس سرویسی که ارائه می دهد و یا بر اساس پروسه هایی که در سیستم اجرا شده اند پورتی را باز کرده تا عملیات بروز رسانی و ... را انجام دهند .و یا شایدم بر اثر وجود یک بد افزار در سیستم عامل شما یک پورتی باز باشد .

ذکر دو مثال ساده بد نیست مثلا شما با نوشتن نشاني ياهو و زدن نام و رمزتان ، پورت ۲۵ بر روی سیستم شما باز میشود و وارد صندوق میشوید در صورتی که این پورت هم توسط مدیر شبکه بسته باشد دیگر این امکان برای شما وجود ندارد .

دومين مثال ساده : شما زماني كه يک صفحه وب (مثل همين صفحه) را باز ميكنيد در واقع پورت ۸۰ شما كه مربوط به http است باز ميشود و شما به وب سايت مورد نظر متصل ميشويد .

متداولترین پورت ها

شناسائی متداولترین پورت هائی که تاکنون مهاجمان با استفاده از آنان حملات خود را سازماندهی نموده اند ، امری لازم و ضروری است . برخی از پورت ها بدفعات و بطور متناوب توسط مهاجمان و به منظور انجام یک تهاجم مورد استفاده قرار گرفته است .

پورتهای ۰ تا ۱۰۲۳ : به این رنج، پرت های رزرو شده می گویند که سیستم عامل از آن جهت ارائه ی سرویس های خود از آن استفاده می نماید .

پورتهای ۱۰۲۴ تا ۴۹۱۵۱ : این رنج از پورت ها بیشتر توسط سازندگان نرم افزار های کاربردی که قدرت ارتباط با شبکه را دارند استفاده می شود مانند مرورگر های اینترنتی و نرم افزار های ارسال و دریافت ایمیل و ...

پورتهای ۴۹۱۵۲ تا ۶۵۵۳۵ : این رنج، که از کم کاربرد ترین پورت ها می باشد بیشتر جهت استفاده از یک سری از سرویس های اینترنتی و بد افزار ها مورد استفاده قرار می گیرد که البته بد افزار های امروزی بیشتر از پرت های بالا استفاده می کنند .

باز بودن پورت های زیر در سیستم های شما به دلیل ویروسی بودن و یا هک شده بودن سیستم شما نیست و شما تا اطلاعات کافی در مورد پورت ها و پروسه های در حال اجرا نداشته باشید نباید هر پورتی را باز یا بسته کنید .

جدول زیر **متداولترین** پورت های آسیب پذیر را تاکنون توسط مهاجمان بکار گرفته شده است ، نشان می دهد :

Port Number	Protocol	Service or Application
7	tcp	echo
11	tcp	systat
19	tcp	chargen
21	tcp	ftp-data
22	tcp	ssh
23	tcp	telnet
25	tcp	smtp
42	tcp	nameserver
43	tcp	whois
49	udp	tacacs
53	udp	dns-lookup
53	tcp	dns-zone
66	tcp	oracle-sqlnet
69	udp	tftp
79	tcp	finger
80	tcp	http
81	tcp	alternative for http
88	tcp	kerberos or alternative for http
109	tcp	pop2
110	tcp	pop3
111	tcp	sunrpc
118	tcp	sqlserv
119	tcp	nntp
135	tcp	ntrpc-or-dec
139	tcp	netbios
143	tcp	imap
161	udp	snmp
162	udp	snmp-trap

179	tcp	bgp
256	tcp	snmp-checkpoint
389	tcp	ldap
396	tcp	netware-ip
407	tcp	timbuktu
443	tcp	https/ssl
445	tcp	ms-smb-alternate
445	udp	ms-smb-alternate
500	udp	ipsec-internet-key-exchange (ike)
513	tcp	rlogin
513	udp	rwho
514	tcp	rshell
514	udp	syslog
515	udp	printer
515	tcp	printer
520	udp	router
524	tcp	netware-n
799	tcp	remotely possible
1080	tcp	socks
1313	tcp	bmc-patrol-db
1352	tcp	notes
1433	tcp	ms-sql
1494	tcp	citrix
1498	tcp	sybase-sql-anywhere
1524	tcp	ingres-lock
1525	tcp	oracle-srv
1527	tcp	oracle-tli
1723	tcp	pptp
1745	tcp	winsock-proxy
2000	tcp	remotely-anywhere
2001	tcp	cisco-mgmt
2049	tcp	nfs
2301	tcp	compaq-web
2447	tcp	openview
2998	tcp	realsecure
3268	tcp	ms-active-dir-global-catalog
3268	udp	ms-active-dir-global-catalog
3300	tcp	bmc-patrol-agent
3306	tcp	mysql
3351	tcp	ssql
3389	tcp	ms-termserv
4001	tcp	cisco-mgmt
4045	tcp	nfs-lockd

5631	tcp	pcanywhere
5800	tcp	vnc
6000	tcp	xwindows
6001	tcp	cisco-mgmt
6549	tcp	apc
6667	tcp	irc
8000	tcp	web
8001	tcp	web
8002	tcp	web
8080	tcp	web
9001	tcp	cisco-xremote
12345	tcp	netbus
26000	tcp	quake
31337	udp	backorifice
32771	tcp	rpc-solaris
32780	udp	snmp-solaris
43188	tcp	Reachout
65301	tcp	pcanywhere-def

برای مشاهده لیست کامل کلیه پورت ها می توانید به آدرس اینترنتی زیر بروید .

www.iana.org/assignments/port-numbers

پویش پورت ها و خطر باز بودن پورت بر روی سیستم شما

پویش یک پورت فرآیندی است که مهاجمان با استفاده از آن قادر به تشخیص وضعیت یک پورت بر روی یک سیستم و یا شبکه می باشند . مهاجمان با استفاده از ابزارهای متفاوت ، اقدام به ارسال داده به پورت های TCP و UDP کامپیوتر هدف می کند و با توجه به نوع بسته ی ارسالی و نوع جواب دریافتی دریافتی قادر به تشخیص این موضوع خواهند بود که کدام پورت ها در حال استفاده بوده و از کدام پورت ها استفاده نمی گردد و اصطلاحا" آنان باز می باشند . مهاجمان در ادامه و بر اساس اطلاعات دریافتی ، بر روی پورت های باز متمرکز شده و حملات خود را بر اساس آنان سازماندهی می نمایند اکثر کرم ها و سایر حملات موفقیت آمیز در اینترنت ، بدلیل وجود نقاط آسیب پذیر در تعدادی اندک از سرویس های سیستم های عامل متداول است .

ممکن است بد افزاری وارد سیستم شما شود و سپس شما آن را شناسایی کنید و به کمک آنتی ویروس یا ... آن را حذف نمایید اما باید بدانید که آن بد افزار بعد از ورود به سیستم شما چه عملیاتی را انجام داده است یکی از اصلی ترین کار هایی که بد افزار ها انجام می دهند معمولا باز کردن پورت هایی بر روس سیستم جهت ارتباط با برنامه نویس و یا سروری خاص می باشد که شما باید بعد از پاک کردن ویروس آن پورت را هم ببندید . اصلا دلیل آمدن بسیاری از Spyware ها بر روی سیستم جهت باز کردن پورت خاص برای رد و بدل کردن اطلاعات از سیستم شما به سرور و بلعکس می باشد .هر پورت باز بر روی سیستم

شما به عنوان یک درب ورودی به سیستم شما محسوب می شود .حتی وقتی که ما میخواهیم وارد یک سایت اینترنتی شویم چون پورت ۸۰ بر روی وب سرور باز بوده ما می توانیم وارد آن شویم هکر ها جهت نفوذ به سیستم شما به جستجوی پورت باز بر روی آن می پردازند و سپس با استفاده از ابزار هایی و با روش هایی خاص به سیستم شما نفوذ می کنند (انشالله در مقالات بعدی به روش های نفوذ به سیستم ها عامل ها می پردازیم)

پیدا کردن پورت های باز بر روی سیستم عامل

برای این کار راه های مختلفی وجود دارد که سعی می کنم تمامی آن را به شما معرفی نمایم .

روش اول استفاده از برنامه ی netstat در سیستم عامل می باشد که در زیر به بررسی این برنامه و فرامین و سویچ های آن می پردازیم .

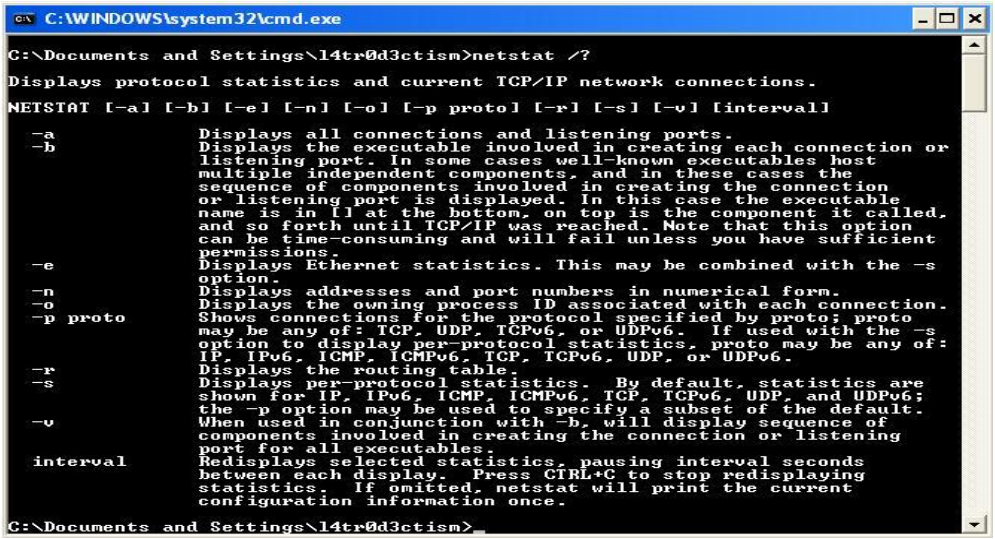
فرمان Netstat

معمولا جزء اولین فرامینی هست که افراد تازه کار با آن آشنا می شوند .حتی باید شنیده باشید که می گویند در هنگام چت اگر بخواهیم ایپی کسی را بدست بیاوریم با فرمان NETSTAT –na می توانیم اینکار را انجام دهیم ؟ خوب دلیل آن این است که این ابزار در سیستم عامل کلیه ی ارتباط ها در شبکه اعم از ایپی هایی که با شما در ارتباط هستند و پورت های مورد نیاز آن و پورت های باز روی سیستم و . . . را به شما نشان می دهد . در اصل این ابزار جهت بر طرف کردن مشکلات به وجود آمده درسیستم عامل ها در شبکه می باشد اما همیشه ، **باید** که مورد سوء استفاده قرار گیرد و این امر بسیار طبیعی می باشد ما در این درس جهت رفع اشکال از آن استفاده می کنیم .پس به معرفی سویچ های آن می پردازیم .

شما می توانید ببینید که ویندوز هم کمک مختصری در مورداین فرمان و سویچ های آن به ما داده است که در help and Support می توانید نمونه ای از آن را با تایپ عبارت netstat ببینید

و همچنین می توانید به CMD بروید و فرمان Netstat را با سویچ /? بکار گیرید تا توضیحی دیگر در مورد فرامین netstat را مشاهده نمایید .

Netstat /? یا Netstat Help



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -v            When used in conjunction with -b, will display sequence of
                components involved in creating the connection or listening
                port for all executables.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.

C:\Documents and Settings\l4tr0d3ctism>_
```

پس در صورتی که به مشکل بر خوردید و دسترسی به اینترنت یا مقالات مرتبط نداشتید از help ویندوز استفاده می کنیم .

Netstat

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    l4tr0d3c-6b8f73:1073   localhost:1074         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:1074   localhost:1073         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3433   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3436   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:4885   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:4899   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:30606  localhost:4885         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:30606  localhost:4899         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:4886   cs213p3.msg.ac4.yahoo.com:5050  ESTABLISHED
  TCP    l4tr0d3c-6b8f73:4900   sip114-p2.voice.ne1.yahoo.com:5050  ESTABLISHED

C:\Documents and Settings\l4tr0d3ctism>
```

این فرمان اگر به تنهایی مورد استفاده قرار گیرد یه ما لیستی نام آدرس هایی که به ما وصل می باشد را نشان می دهد

در این صفحه شما چند سربرگ را می بینید .

Porto : نوع پروتکلی که کانکشن از آن استفاده می کند که دو حالت دارد (UDP – TCP)

Local Address : لیست نام کانکشن و یا ایپی های سیستم خودمان را نمایش می دهد و در مقابل آن بعد از علامت : پورت هایی که کانکشن از آن استفاده می کند را نمایش می دهد .

Foreign Address : نام یا ایپی هایی که به ما متصل هستند و همچنین پورت هایی که آن ها با استفاده از آن به کامپیوتر ما متصل شده است را نمایش می دهد .

Stat: وضعیت کانکشن های Tcp را به ما نشان می دهد که ممکن است حالت های زیر را داشته باشد

- **CLOSE_WAIT** : کانکشن در حال بسته شدن است .
- **CLOSED** : کانکشن بسته شده است .
- **ESTABLISHED** : کانکشن به کامپیوتر شما ارتباط برقرار کرده است .
- **FIN_WAIT_1** : نشان می دهد که اتصال در حال حاضر فعال است اما مورد استفاده قرار نگرفته است .
- **FIN_WAIT_2** : نشان می دهد که کانکشن فقط یک سیگنال Fin از سرور دریافت کرده است .
- **LAST_ACK** : نشان می دهد که سرور در حال ارسال Fin می باشد .
- **LISTEN** : نشان می دهد که اتصال آماده ی پذیرفتن اتصال می باشد .
- **SYN_RECEIVED** : نشان می دهد که سرور فقط یک سیگنال SYN را از Client دریافت کرده .
- **SYN_SEND** : نشان می دهد که این اتصال باز و فعال است .
- **TIMED_WAIT :** نشان می دهد که اتصال بین Client و Server برقرار است اما در حال حاضر مورد استفاده قرار نگرفته است .
-

سویچ a–

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    l4tr0d3c-6b8f73:epmap  l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:microsoft-ds  l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:1935   l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:5101   l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:7955   l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:12882  l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:1031   l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:1043   localhost:1044         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:1044   localhost:1043         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3043   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3048   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3335   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3347   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:18936  l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:30606  l4tr0d3c-6b8f73:0      LISTENING
  TCP    l4tr0d3c-6b8f73:30606  localhost:3044         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3335         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:30606  localhost:3347         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3336   cs219p1.msg.ac4.yahoo.com:5050  ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3348   sip111-p1.voice.ne1.yahoo.com:5050  ESTABLISHED
  UDP    l4tr0d3c-6b8f73:microsoft-ds  *:*
  UDP    l4tr0d3c-6b8f73:isakmp  *:*
  UDP    l4tr0d3c-6b8f73:1082   *:*
  UDP    l4tr0d3c-6b8f73:1121   *:*
  UDP    l4tr0d3c-6b8f73:2098   *:*
  UDP    l4tr0d3c-6b8f73:2152   *:*
  UDP    l4tr0d3c-6b8f73:4500   *:*
  UDP    l4tr0d3c-6b8f73:ntp    *:*
  UDP    l4tr0d3c-6b8f73:1090   *:*
  UDP    l4tr0d3c-6b8f73:1900   *:*
  UDP    l4tr0d3c-6b8f73:ntp    *:*
  UDP    l4tr0d3c-6b8f73:1900   *:*

C:\Documents and Settings\l4tr0d3ctism>color f
```

این فرمان لیستی از تمامی ارتباط هایی را که در سه حالت TIMED_WAIT و ESTABLISHED و LISTENing را برای شما می آورد

سویچ n–

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1043         127.0.0.1:1044         ESTABLISHED
  TCP    127.0.0.1:1044         127.0.0.1:1043         ESTABLISHED
  TCP    127.0.0.1:3059         127.0.0.1:12882        TIME_WAIT
  TCP    127.0.0.1:3062         127.0.0.1:12882        TIME_WAIT
  TCP    127.0.0.1:3335         127.0.0.1:30606        ESTABLISHED
  TCP    127.0.0.1:3347         127.0.0.1:30606        ESTABLISHED
  TCP    127.0.0.1:30606        127.0.0.1:3335         ESTABLISHED
  TCP    127.0.0.1:30606        127.0.0.1:3347         ESTABLISHED
  TCP    192.168.1.2:3336       67.195.186.84:5050     ESTABLISHED
  TCP    192.168.1.2:3348       98.138.26.101:5050     ESTABLISHED

C:\Documents and Settings\l4tr0d3ctism>
```

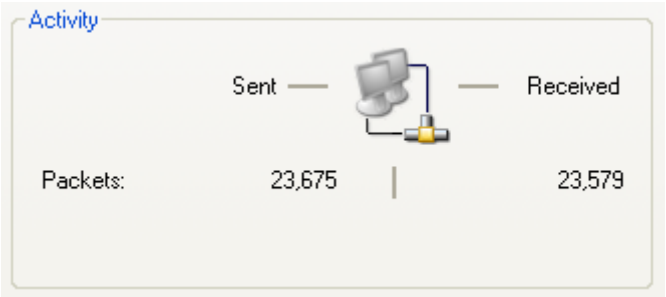
این سویچ مانند سویچ a- بوده لیستی از **اپی های** کانکشن ها را برای ما می آورد

ویچ e–

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      1892410          1730639
Unicast packets              19091            20247
Non-unicast packets            213              205
Discards                         0                0
Errors                           0                0
Unknown protocols                0

C:\Documents and Settings\l4tr0d3ctism>
```

این سویچ می تواند حجم کلیه ی پاکتهای فرستاده شده از طرف کامپیوتر شما و دریافت شده از طرف کانکشن ها را به بایت محاسبه کند و می تواند تعداد بایتهای متناظر با هر نوع انتقال شبکه ای را گزارش داد.

البته می توان با رفتن به properties کانکشن خودمان در سربرگ Generall هم آن را مشاهده کرد



سویچ o- یا v-

```
Command Prompt
C:\Documents and Settings\l4tr0d3ctism>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    l4tr0d3c-6b8f73:1043   localhost:1044         ESTABLISHED     4048
  TCP    l4tr0d3c-6b8f73:1044   localhost:1043         ESTABLISHED     4048
  TCP    l4tr0d3c-6b8f73:3103   localhost:12882        TIME_WAIT       0
  TCP    l4tr0d3c-6b8f73:3106   localhost:12882        TIME_WAIT       0
  TCP    l4tr0d3c-6b8f73:3107   localhost:30606        FIN_WAIT_2      680
  TCP    l4tr0d3c-6b8f73:3335   localhost:30606        ESTABLISHED     4048
  TCP    l4tr0d3c-6b8f73:3347   localhost:30606        ESTABLISHED     4048
  TCP    l4tr0d3c-6b8f73:30606  localhost:3107         CLOSE_WAIT      388
  TCP    l4tr0d3c-6b8f73:30606  localhost:3335         ESTABLISHED     388
  TCP    l4tr0d3c-6b8f73:30606  localhost:3347         ESTABLISHED     388
  TCP    l4tr0d3c-6b8f73:3108   KD111111111111.ppp-bb.dion.ne.jp:http  SYN_SENT
       388
  TCP    l4tr0d3c-6b8f73:3336   cs219p1.msg.ac4.yahoo.com:5050  ESTABLISHED
388
  TCP    l4tr0d3c-6b8f73:3348   sip111-p1.voice.ne1.yahoo.com:5050  ESTABLISHED
    388

C:\Documents and Settings\l4tr0d3ctism>
```

این ۲ فرمان برای ما لیستی از کانکشن ها و PID های آن ها را نمایش دهد . PIDها در اصل شماره پروسه ایست که جهت ارتباط با اینترنت از این کانکشن استفاده می کند .

سویچ s–

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -s

IPv4 Statistics

  Packets Received                   = 19240
  Received Header Errors             = 0
  Received Address Errors            = 10
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 1
  Received Packets Delivered         = 19226
  Output Requests                    = 20425
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                           Received    Sent
  Messages                 422         10
  Errors                   0           0
  Destination Unreachable  417         4
  Time Exceeded            0           0
  Parameter Problems       0           0
  Source Quenches          0           0
  Redirects                0           0
  Echos                    2           4
  Echo Replies             3           2
  Timestamps               0           0
  Timestamp Replies        0           0
  Address Masks            0           0
  Address Mask Replies     0           0

TCP Statistics for IPv4

  Active Opens                        = 2251
  Passive Opens                       = 1177
  Failed Connection Attempts          = 256
  Reset Connections                   = 187
  Current Connections                 = 0
  Segments Received                   = 17067
  Segments Sent                       = 16905
  Segments Retransmitted              = 514

UDP Statistics for IPv4

  Datagrams Received    = 1587
  No Ports              = 599
  Receive Errors        = 2
  Datagrams Sent        = 2994

C:\Documents and Settings\l4tr0d3ctism>
```

این فرمان جهت محاسبات و آمارگیری از پروتکلهای کانکشن ها می باشد .به صورت پیش فرض سه پروتکل TCP, UDP, ICMP را جهت محاسبات عددی که مانند میزان ارسال و دریافت هست را محاسبه می کند ولی اگر IPv6 در ویندوز نصب شود در این صورت TCP over IPv6, UDP over IPv6, ICMPv6, IPv6 را نیز محاسبه می نامید .

سویچ p-

```
Command Prompt
C:\Documents and Settings\l4tr0d3ctism>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    l4tr0d3c-6b8f73:1043   localhost:1044         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:1044   localhost:1043         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3145   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3146   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3147   localhost:30606        FIN_WAIT_2
  TCP    l4tr0d3c-6b8f73:3335   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3347   localhost:30606        ESTABLISHED
  TCP    l4tr0d3c-6b8f73:30606  localhost:3139         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3141         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3147         CLOSE_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3335         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:30606  localhost:3347         ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3148   KD111111111111.ppp-bb.dion.ne.jp:http  SYN_SENT
  TCP    l4tr0d3c-6b8f73:3336   cs219p1.msg.ac4.yahoo.com:5050  ESTABLISHED
  TCP    l4tr0d3c-6b8f73:3348   sip111-p1.voice.ne1.yahoo.com:5050  ESTABLISHED

C:\Documents and Settings\l4tr0d3ctism>_
```

این فرمان می تواند لیستی از تمامی کانکشن هایی را که از پروتکل های خاصی استفاده می کنند را برای ما نمایش دهد پروتکل ها شامل **tcp** و **udp** و **tcpv6** یا **udpv6** شود.

سویچ r–

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\l4tr0d3ctism>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...50 e5 49 bf 6b 36 ...... Realtek PCIe GBE Family Controller - Packet Sche
duler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.2      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0      192.168.1.2     192.168.1.2      20
      192.168.1.2  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.1.255  255.255.255.255      192.168.1.2     192.168.1.2      20
        224.0.0.0        240.0.0.0      192.168.1.2     192.168.1.2      20
  255.255.255.255  255.255.255.255      192.168.1.2     192.168.1.2       1
Default Gateway:       192.168.1.1
===========================================================================
Persistent Routes:
  None

C:\Documents and Settings\l4tr0d3ctism>_
```

Netstat –r

این فرمان برای تست حالات اتصالات و محتویات جدول های مسیریابی شبکه ی که در آن حضور داریم (TCP/IP) را نشان می دهد که شامل Interface , Defoult Gateway , Netmask و Metric می باشد .

سویچ b–

```
Command Prompt

C:\Documents and Settings\l4tr0d3ctism>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    l4tr0d3c-6b8f73:1218   localhost:1219         ESTABLISHED     3368
  [firefox.exe]

  TCP    l4tr0d3c-6b8f73:1219   localhost:1218         ESTABLISHED     3368
  [firefox.exe]

  TCP    l4tr0d3c-6b8f73:1220   localhost:1221         ESTABLISHED     3368
  [firefox.exe]

  TCP    l4tr0d3c-6b8f73:1221   localhost:1220         ESTABLISHED     3368
  [firefox.exe]

  TCP    l4tr0d3c-6b8f73:1222   localhost:12882        TIME_WAIT       0
  TCP    l4tr0d3c-6b8f73:1223   localhost:12882        TIME_WAIT       0

C:\Documents and Settings\l4tr0d3ctism>_
```

این فرمان لیستی از برنامه هایی که در سیستم عامل از پورت های خاصی استفاده می کنند را برایمان میاورد .

همچنین می توانیم در برنامه ی netstat با در کنار هم قرار دادن سویچ های برنامه به نتایج جامعتر و مفید تری دسترسی پیدا کنیم .

Netstat –s –p "tCp"

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -s -p TCP

TCP Statistics for IPv4

  Active Opens                        = 2273
  Passive Opens                       = 1191
  Failed Connection Attempts          = 256
  Reset Connections                   = 187
  Current Connections                 = 0
  Segments Received                   = 17231
  Segments Sent                       = 17075
  Segments Retransmitted              = 514

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    l4tr0d3c-6b8f73:3548   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:3551   localhost:12882        TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3542         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3543         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3546         TIME_WAIT
  TCP    l4tr0d3c-6b8f73:30606  localhost:3549         TIME_WAIT

C:\Documents and Settings\l4tr0d3ctism>_
```

این فرمان لیستی از کانکشن هایی که از پروتکل TCP استفاده می کند و همچنین محاسبات مربوط به کانکشن ها را ر کنار هم نشان می دهد .

Netstat -an

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1935           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7955           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12882          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1031         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1171         127.0.0.1:12882        TIME_WAIT
  TCP    127.0.0.1:1172         127.0.0.1:12882        TIME_WAIT
  TCP    127.0.0.1:18936        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:30606        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*

C:\Documents and Settings\l4tr0d3ctism>
```

این فرمان لیستی کامل از تمامی کانکشن های مرتبط با ما و پورت های باز روی سیستم را برایمان می آورد .یکی ار فرامین مهم Netstatمی باشد (قابل توجه جوجه هکرها)

Netstat -ano

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\14tr0d3ctism>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1935           0.0.0.0:0              LISTENING       176
  TCP    0.0.0.0:7955           0.0.0.0:0              LISTENING       176
  TCP    0.0.0.0:12882          0.0.0.0:0              LISTENING       176
  TCP    127.0.0.1:1044         0.0.0.0:0              LISTENING       2988
  TCP    127.0.0.1:3702         127.0.0.1:12882        TIME_WAIT       0
  TCP    127.0.0.1:3705         127.0.0.1:12882        TIME_WAIT       0
  TCP    127.0.0.1:18936        0.0.0.0:0              LISTENING       176
  TCP    127.0.0.1:22678        0.0.0.0:0              LISTENING       1544
  TCP    127.0.0.1:30606        0.0.0.0:0              LISTENING       2032
  TCP    127.0.0.1:30606        127.0.0.1:3696         TIME_WAIT       0
  TCP    127.0.0.1:30606        127.0.0.1:3700         TIME_WAIT       0
  TCP    127.0.0.1:30606        127.0.0.1:3703         TIME_WAIT       0
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    1044
  UDP    0.0.0.0:1026           *:*                                    1520
  UDP    0.0.0.0:1054           *:*                                    1520
  UDP    0.0.0.0:1513           *:*                                    1520
  UDP    0.0.0.0:1552           *:*                                    1520
  UDP    0.0.0.0:4500           *:*                                    1044
  UDP    127.0.0.1:123          *:*                                    1476
  UDP    127.0.0.1:1900         *:*                                    1676
  UDP    127.0.0.1:1975         *:*                                    1112
  UDP    127.0.0.1:1998         *:*                                    1544
  UDP    127.0.0.1:2118         *:*                                    1936
  UDP    127.0.0.1:2145         *:*                                    3392
  UDP    127.0.0.1:2148         *:*                                    596
  UDP    127.0.0.1:3185         *:*                                    2300
  UDP    127.0.0.1:3508         *:*                                    1204
  UDP    127.0.0.1:3576         *:*                                    452
  UDP    192.168.1.2:123        *:*                                    1476
  UDP    192.168.1.2:137        *:*                                    4
  UDP    192.168.1.2:138        *:*                                    4
  UDP    192.168.1.2:1900       *:*                                    1676

C:\Documents and Settings\14tr0d3ctism>_
```

این فرمان لیستی از تمامی اتصالات را به کامپیوتر ما + ایدی پروسه ی استفاده کننده از اتصال مورد نظر را به ما می دهد .

Netstat –anobv

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\14tr0d3ctism>netstat -anobv

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1340
  c:\windows\system32\WS2_32.dll
  C:\WINDOWS\system32\RPCRT4.dll
  c:\windows\system32\rpcss.dll
  C:\WINDOWS\system32\svchost.exe
  C:\WINDOWS\system32\ADVAPI32.dll
  [svchost.exe]

  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  -- unknown component(s) --
  [System]

  TCP    0.0.0.0:1935           0.0.0.0:0              LISTENING       176
  C:\WINDOWS\system32\WS2_32.DLL
  C:\Program Files\PANDORA.TV\PanService\PanStreamer.dll
  C:\Program Files\PANDORA.TV\PanService\PandoraService.exe
  C:\WINDOWS\system32\kernel32.dll
  [PandoraService.exe]

  TCP    0.0.0.0:7955           0.0.0.0:0              LISTENING       176
  C:\WINDOWS\system32\WS2_32.DLL
  C:\Program Files\PANDORA.TV\PanService\proxy.dll
  C:\Program Files\PANDORA.TV\PanService\PandoraService.exe
  C:\WINDOWS\system32\kernel32.dll
  [PandoraService.exe]

  TCP    0.0.0.0:12882          0.0.0.0:0              LISTENING       176
  C:\WINDOWS\system32\WS2_32.DLL
  C:\Program Files\PANDORA.TV\PanService\PandoraService.exe
  C:\WINDOWS\system32\kernel32.dll
  [PandoraService.exe]

  TCP    127.0.0.1:1044         0.0.0.0:0              LISTENING       2988
  C:\WINDOWS\System32\WS2_32.dll
  C:\WINDOWS\System32\alg.exe
  C:\WINDOWS\system32\RPCRT4.dll
  C:\WINDOWS\system32\ole32.dll
  [alg.exe]

  TCP    127.0.0.1:18936        0.0.0.0:0              LISTENING       176
  C:\WINDOWS\system32\WS2_32.DLL
  C:\Program Files\PANDORA.TV\PanService\PanStreamer.dll
  C:\Program Files\PANDORA.TV\PanService\PandoraService.exe
  C:\WINDOWS\system32\kernel32.dll
  [PandoraService.exe]

  TCP    127.0.0.1:22678        0.0.0.0:0              LISTENING       1544
  [BabylonTC.exe]

  TCP    127.0.0.1:30606        0.0.0.0:0              LISTENING       2032
  C:\WINDOWS\system32\WS2_32.dll
  C:\Program Files\ESET\ESET Smart Security\ekrnEpfw.dll
  C:\Program Files\ESET\ESET Smart Security\ekrn.exe
  C:\WINDOWS\system32\kernel32.dll
  [ekrn.exe]
```

C:\WINDOWS\system32\cmd.exe

```
TCP    192.168.1.2:139        0.0.0.0:0              LISTENING       4
-- unknown component(s) --
[System]

TCP    127.0.0.1:3705         127.0.0.1:12882        TIME_WAIT       0
TCP    127.0.0.1:3708         127.0.0.1:12882        TIME_WAIT       0
TCP    127.0.0.1:30606        127.0.0.1:3703         TIME_WAIT       0
TCP    127.0.0.1:30606        127.0.0.1:3706         TIME_WAIT       0
UDP    0.0.0.0:1552           *:*                                    1520
C:\WINDOWS\system32\mswsock.dll
c:\windows\system32\WS2_32.dll
c:\windows\system32\DNSAPI.dll
c:\windows\system32\dnsrslvr.dll
C:\WINDOWS\system32\RPCRT4.dll
[svchost.exe]

UDP    0.0.0.0:445            *:*                                    4
-- unknown component(s) --
[System]

UDP    0.0.0.0:4500           *:*                                    1044
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\oakley.DLL
C:\WINDOWS\system32\LSASRV.dll
C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\kernel32.dll
[lsass.exe]

UDP    0.0.0.0:500            *:*                                    1044
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\oakley.DLL
C:\WINDOWS\system32\LSASRV.dll
C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\kernel32.dll
[lsass.exe]

UDP    0.0.0.0:1026           *:*                                    1520
C:\WINDOWS\system32\mswsock.dll
c:\windows\system32\WS2_32.dll
c:\windows\system32\DNSAPI.dll
c:\windows\system32\dnsrslvr.dll
C:\WINDOWS\system32\RPCRT4.dll
[svchost.exe]

UDP    0.0.0.0:1054           *:*                                    1520
C:\WINDOWS\system32\mswsock.dll
c:\windows\system32\WS2_32.dll
c:\windows\system32\DNSAPI.dll
c:\windows\system32\dnsrslvr.dll
C:\WINDOWS\system32\RPCRT4.dll
[svchost.exe]

UDP    0.0.0.0:1513           *:*                                    1520
C:\WINDOWS\system32\mswsock.dll
c:\windows\system32\WS2_32.dll
c:\windows\system32\DNSAPI.dll
c:\windows\system32\dnsrslvr.dll
C:\WINDOWS\system32\RPCRT4.dll
[svchost.exe]

UDP    127.0.0.1:3185         *:*                                    2300
```

C:\WINDOWS\system32\cmd.exe

```
UDP    127.0.0.1:3185         *:*                                    2300
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[wmplayer.exe]

UDP    127.0.0.1:2118         *:*                                    1936
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[IEXPLORE.EXE]

UDP    127.0.0.1:1975         *:*                                    1112
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[Babylon.exe]

UDP    127.0.0.1:3576         *:*                                    452
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[IEXPLORE.EXE]

UDP    127.0.0.1:123          *:*                                    1476
c:\windows\system32\WS2_32.dll
c:\windows\system32\w32time.dll
ntdll.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]

UDP    127.0.0.1:1900         *:*                                    1676
c:\windows\system32\WS2_32.dll
c:\windows\system32\ssdpsrv.dll
ntdll.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]

UDP    127.0.0.1:3508         *:*                                    1204
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[HelpHost.exe]

UDP    127.0.0.1:1998         *:*                                    1544
C:\WINDOWS\system32\WS2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[BabylonTG.exe]

UDP    127.0.0.1:2148         *:*                                    596
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[IEXPLORE.EXE]

UDP    127.0.0.1:2145         *:*                                    3392
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\WININET.dll
C:\WINDOWS\system32\kernel32.dll
[IEXPLORE.EXE]
```

این فرمان هم یکی از فرامین مهم و پرکاربرد Netstat می باشد که در آن لیستی از برنامه ها و فایل های کتاب خانه ای که از پورتی خاص و اتصالی خاص همراه با ایدی پروسه ی آنها و آدرس فایل ها را برایمان لیست می کند . این فرمان بیشتر جهت تشخیص بد افزار بر روی سیستم موثر می باشد .

|find /I "listening"

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -an |find /i "listening"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1935           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7955           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12882          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1044         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:18936        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:22678        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:30606        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING

C:\Documents and Settings\l4tr0d3ctism>_
```

با استفاده از این فرمان در جلوی سویچ ها در برنامه ی Netstat می توانید دنبال یک کانکشن که در یک حالت خاص قرار دارد باشید .

|find /I "1544"

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -ano |find /i "1544"
  TCP    127.0.0.1:22678        0.0.0.0:0              LISTENING       1544
  UDP    127.0.0.1:1998         *:*                                    1544

C:\Documents and Settings\l4tr0d3ctism>
```

با استفاده از این فرمان هم می توانید بفهمید که مثلا پروسه ای خاص از چه پرت و یا کانکشنی استفاده می کند.

> "C:/example.txt"

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>netstat -an > "c:/openports.txt"

C:\Documents and Settings\l4tr0d3ctism>_
```

می توانید با به کار گیری این فرمان در جلوی سویچ در برنامه Netstat خروجی را در یک فایل متنی به شکل زیر بیاندازید .

```
openports - Notepad
File  Edit  Format  View  Help

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1935           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7955           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12882          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1044         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3602         127.0.0.1:30606        TIME_WAIT
  TCP    127.0.0.1:3617         127.0.0.1:30606        TIME_WAIT
```

حال شما فرامین Netstat را می دانید و می توانید از آن استفاده نمایید

شما می توانید که لیستی از PId ها یی که از کانکشنی خاص استفاده می کنند را بدست آوردید (Netstat –ano) سپس باید بدانید که PiD یا همان مورد نظر مربوط به کدام پروسه ی در حال اجرا می باشد برای این کاز از چند روش می توانید استفاده کنید .

فرمان Tasklist

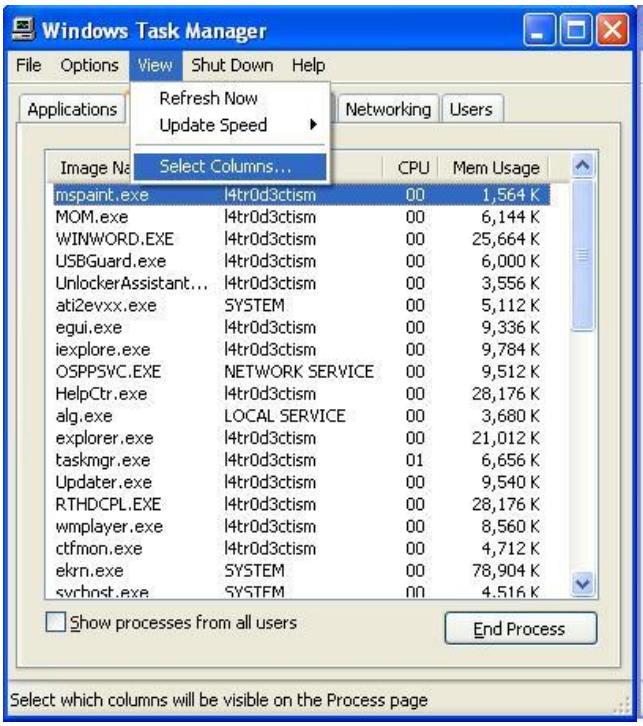
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\l4tr0d3ctism>Tasklist

Image Name                     PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process              0 Console                0         28 K
System                           4 Console                0        240 K
smss.exe                      1212 Console                0        420 K
csrss.exe                     1316 Console                0      6,384 K
winlogon.exe                  1360 Console                0      6,696 K
services.exe                  1404 Console                0      3,792 K
lsass.exe                     1416 Console                0      1,396 K
ati2evxx.exe                  1580 Console                0      3,544 K
svchost.exe                   1596 Console                0      5,024 K
svchost.exe                   1696 Console                0      4,576 K
svchost.exe                   1736 Console                0     24,712 K
svchost.exe                   1856 Console                0      3,096 K
svchost.exe                   1884 Console                0      4,828 K
spoolsv.exe                   2004 Console                0      4,956 K
ati2evxx.exe                   180 Console                0      5,096 K
BWMeterConSvc.exe              268 Console                0      2,004 K
ekrn.exe                       292 Console                0     77,484 K
PandoraService.exe             404 Console                0      9,836 K
alg.exe                       1096 Console                0      3,648 K
wscntfy.exe                   1040 Console                0      3,332 K
explorer.exe                  1092 Console                0     21,040 K
RTHDCPL.EXE                   3656 Console                0     25,396 K
egui.exe                      3712 Console                0      6,240 K
USBGuard.exe                  3792 Console                0      5,744 K
CloneCDTray.exe               3804 Console                0      3,816 K
UnlockerAssistant.exe         3812 Console                0      3,604 K
VCDDaemon.exe                 3840 Console                0      4,204 K
ctfmon.exe                    3852 Console                0      4,384 K
IDMan.exe                     3868 Console                0     11,944 K
hackmon.exe                   3888 Console                0      4,968 K
MOM.exe                       1324 Console                0      7,392 K
CCC.exe                       2064 Console                0      7,492 K
IEMonitor.exe                 2072 Console                0      4,524 K
Ymsgr_tray.exe                2248 Console                0      7,092 K
WINWORD.EXE                   1636 Console                0     67,660 K
OSPPSVC.EXE                   2720 Console                0      9,460 K
HelpCtr.exe                    492 Console                0      5,352 K
HelpSvc.exe                   2784 Console                0     12,136 K
HelpHost.exe                  1516 Console                0      7,344 K
svchost.exe                   3432 Console                0      4,416 K
iexplore.exe                  2468 Console                0      3,536 K
iexplore.exe                  2408 Console                0     27,600 K
firefox.exe                   3368 Console                0     56,788 K
Babylon.exe                   2436 Console                0     37,004 K
BabylonTC.exe                 2656 Console                0     71,196 K
cmd.exe                       2984 Console                0      2,792 K
tasklist.exe                  3996 Console                0      5,444 K
wmiprvse.exe                  1236 Console                0      5,800 K

C:\Documents and Settings\l4tr0d3ctism>
```

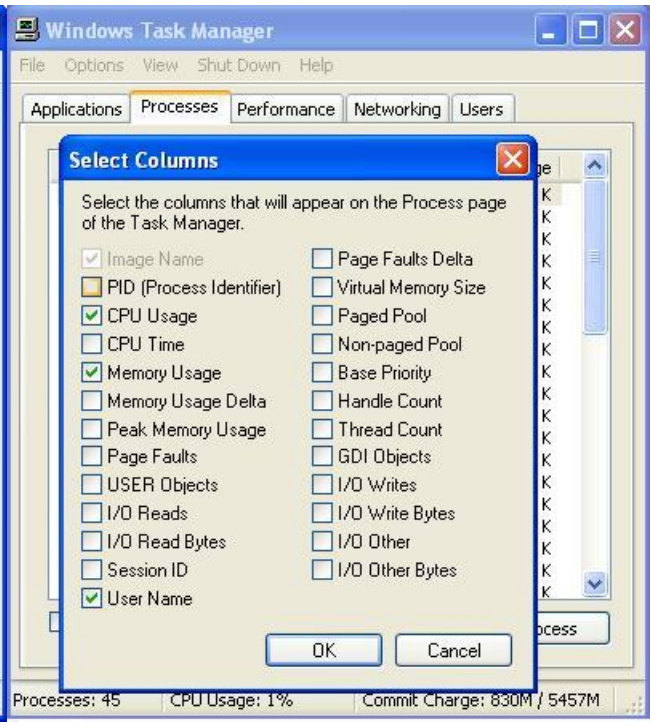
این فرمان لیستی از processes های در حال اجرا ، همراه با PID آنها را برایمان نمایش می دهد و ما می توانیم بفهمیم که PID هایی که با استفاده از فرمان Netstat –ano نمایش داده می شود مربوط به کدام پروسه می باشد و بفهمیم چه پروسه ای از چه پورتهایی استفاده می کند .

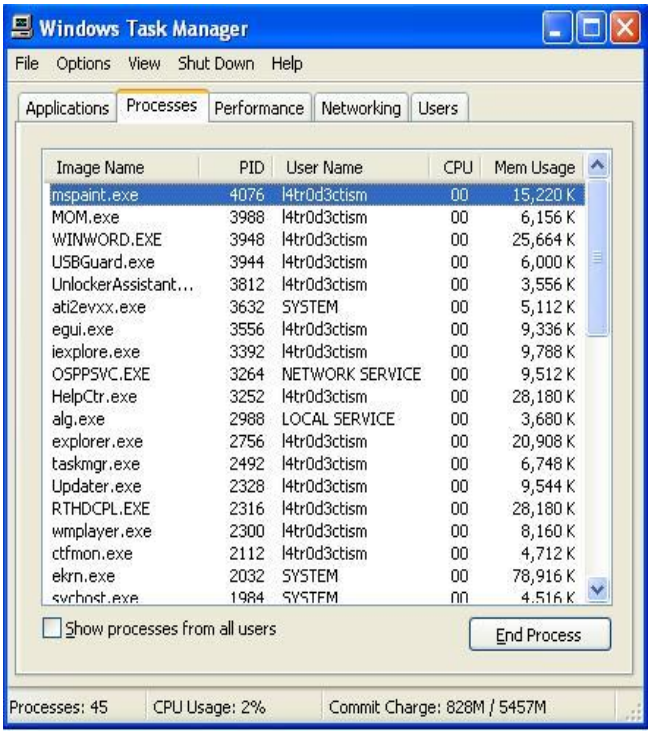
همچنین جهت نمایش PIDسرویس ها هم می توانید از فرمان tasklist /svc استفاده کنید .به شکل زیر

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\l4tr0d3ctism>tasklist /svc

Image Name                     PID Services
========================= ====== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       856 N/A
csrss.exe                      944 N/A
winlogon.exe                   988 N/A
services.exe                  1032 Eventlog, PlugPlay
lsass.exe                     1044 PolicyAgent, ProtectedStorage, SamSs
ati2evxx.exe                  1220 Ati HotKey Poller
svchost.exe                   1236 DcomLaunch, TermService
svchost.exe                   1340 RpcSs
svchost.exe                   1476 AudioSrv, BITS, Browser, CryptSvc, Dhcp,
                                   dmserver, ERSvc, EventSystem,
                                   FastUserSwitchingCompatibility, helpsvc,
                                   LanmanServer, lanmanworkstation, Netman,
                                   Nla, RasMan, Schedule, seclogon, SENS,
                                   SharedAccess, ShellHWDetection, srservice,
                                   TapiSrv, Themes, TrkWks, W32Time, winmgmt,
                                   wscsvc, wuauserv, WZCSVC
svchost.exe                   1520 Dnscache
svchost.exe                   1676 LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe                   1872 Spooler
ekrn.exe                      2032 ekrn
PandoraService.exe             176 PanService
alg.exe                       2988 ALG
OSPPSVC.EXE                   3264 osppsvc
svchost.exe                   1984 stisvc
wscntfy.exe                    612 N/A
ati2evxx.exe                  3632 N/A
explorer.exe                  2756 N/A
RTHDCPL.EXE                   2316 N/A
egui.exe                      3556 N/A
MOM.exe                       3988 N/A
USBGuard.exe                  3944 N/A
CloneCDTray.exe                300 N/A
Babylon.exe                   1112 N/A
UnlockerAssistant.exe         3812 N/A
Updater.exe                   2328 N/A
ctfmon.exe                    2112 N/A
CCC.exe                       1492 N/A
BabylonTC.exe                 1544 N/A
iexplore.exe                  3392 N/A
iexplore.exe                  1936 N/A
iexplore.exe                   596 N/A
WINWORD.EXE                   3948 N/A
wmplayer.exe                  2300 N/A
mspaint.exe                   4076 N/A
cmd.exe                       1840 N/A
HelpCtr.exe                   3252 N/A
HelpSvc.exe                   1352 N/A
HelpHost.exe                  1204 N/A
iexplore.exe                   452 N/A
tasklist.exe                  3368 N/A
wmiprvse.exe                  1736 N/A

C:\Documents and Settings\l4tr0d3ctism>
```

همچنین می توان جهت دیدن PID پروسه ها هم می توانید در Taskmanager از منوی View گزینه ی select columns و سپس PID را انتخاب کنید .





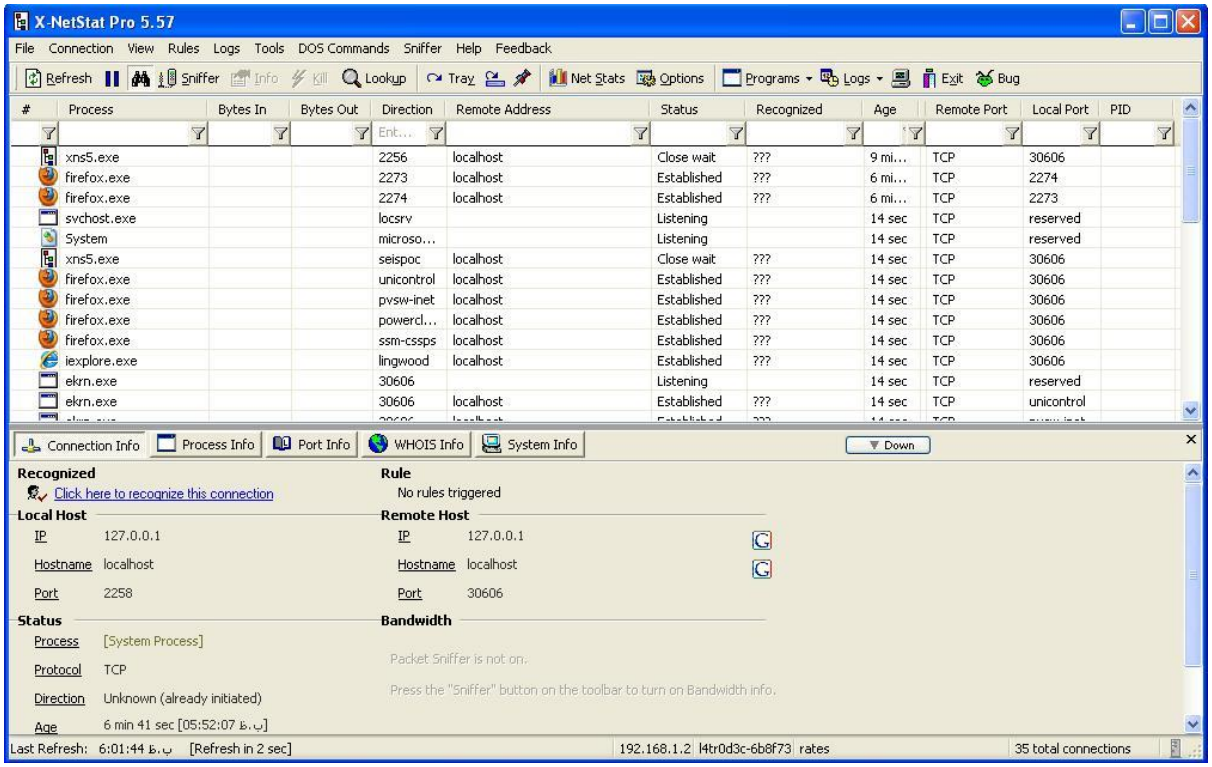


در نهایت شما می توانید بفهمید که چه پروسه ای از چه پورتی استفاده می کند و در صورتی که مشاهده می کنید که پورت هایی بر روس سیستم شما فعال هستند که هیچ پروسه ای از آن استفاده نمی کن و یا برنامه ای نا شناس از آن استفاده می کند می توانید آن را ببندید چون امکان دارد بد افزاری بر روی سیستم شما نصب شده باشد .

با استفاده از نرم افزار X-netstat

این نرم افزار هم در اصل ورژن گرافیکی برنامه Netstat ویندوز می باشد که کار را برای ما آسان تر کرده باشد و همه ی اطلاعات مورد نیاز را به طور کامل برای ما شرح داده باشد

رد زیر نمایی از محاین برنامه گذاشته می شود .



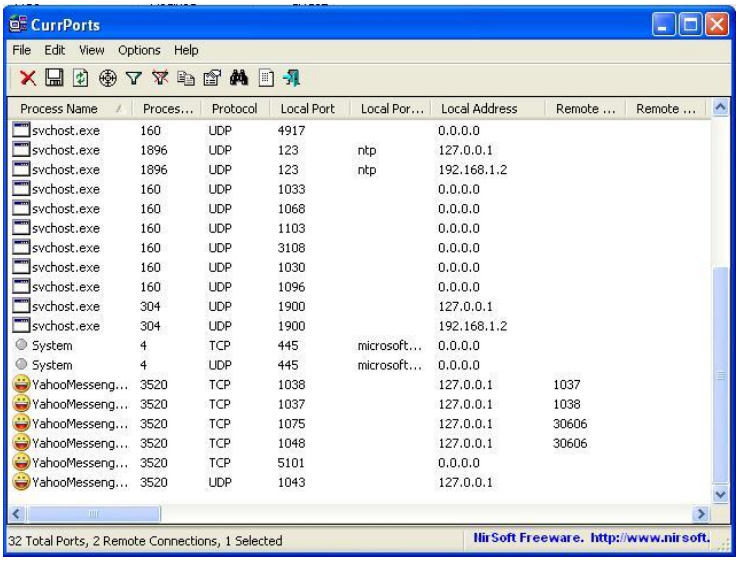
در صورتی که شما با فرامین Netstat که در بالا شرح داده شد آشنا باشید و آن را به درستی یاد گرفته باشید می توانید با این ابزار هم به سادگی کار کنید .

قابلیت های کلیدی نرم افزار X-Netstat Professional:

- بدست آوردن IP افراد در اینترنت
- امکان مشاهده آی پی قربانی تنها با ارسال یک پی ام از طرف وی
- قابلیت بدست آوردن اطلاعات قربانی همچون نام کشور، نام شهر، نام ISP، شماره تلفن و ... او
- آگاه سازی کاربر از IP ها و پورت های درحال استفاده
- جلوگیری از اتصالات خروجی
- نسخه قابل چاپ و اتصال ذخیره جدول
- امکان ورود به سیستم فعالیت XNS
- قابلیت جستجو و فیلتر اطلاعات
- امکان پردازش اطلاعات دریافتی
- امکان آگاهی از پورت ای بازی که مخصوص تروجان خاص
- و ...

نرم افزار Cureport

نرم افزار Cport محصول شرکت nirsoft ابزاری جهت نمایش لیستی از process ها پورت هایی که مورد استفاده ی آنها قرار می گیرد و در شبکه در حال فعالیت هستند می باشد این برنامه ابزار مفیدی برای شناسایی بد افزار ها می باشد

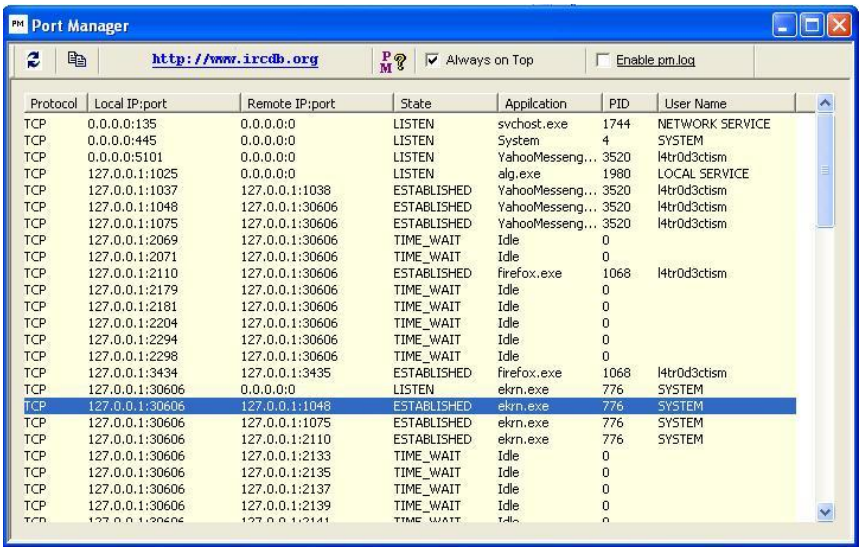


می توانید این برنامه را در آدرس زیر دریافت کنید

http://www.nirsoft.net/utils/cports.zip

برنامه Port Manager

این برنامه هم یکی دیگر از Task manager ها بوده جهت شناسایی پورت های باز روی سیستم به کار برده می شود .که بسیاری از موارد قوی تر از Cport عمل می کند .



http://portmanager.smike.ru/pm.zip

با استفاده از Scanner ها

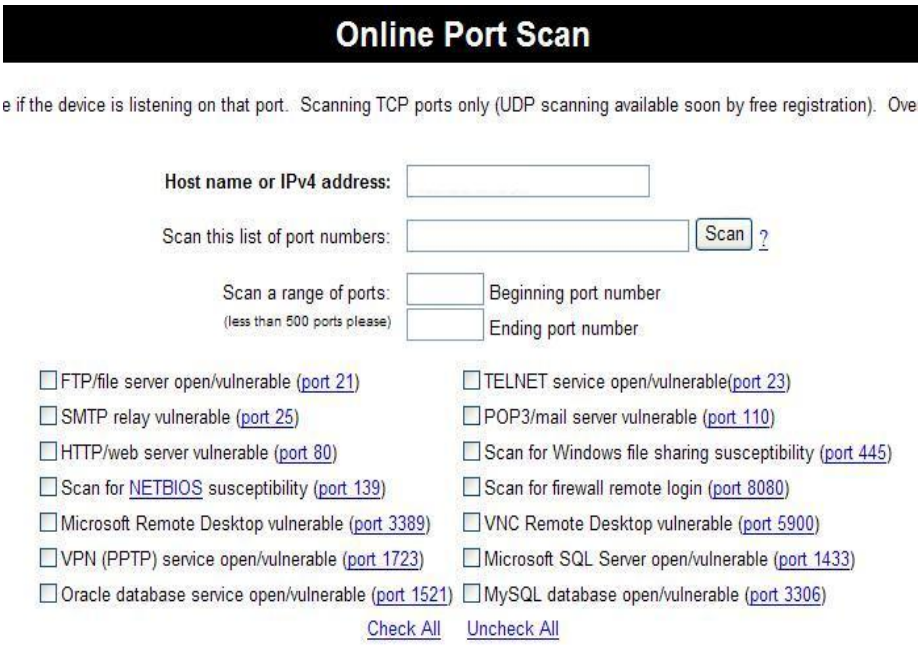
انواع مختلفی از اسکنر ها وجود دارد که چند نمونه از آن را در زیر آموزش می دهیم .

Online port Scanner

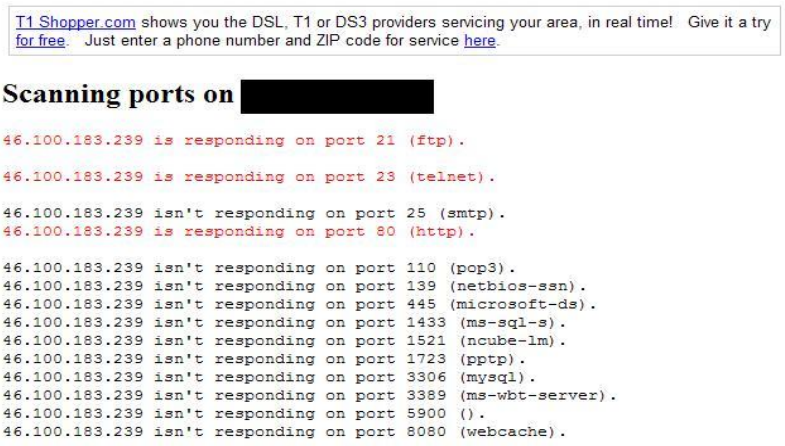
در اینترنت هم یکسری سرویس های آنلاین وجود دارد که با دادن ایپی یک کلاینت و یا سایت و یا با استفاده از نام دامنه ی اینترنتی سایت به پیدا کردن پورت های باز در ایپی داده شده بپردازد . در زیر نمونه ای را به شما معرفی می کنیم .

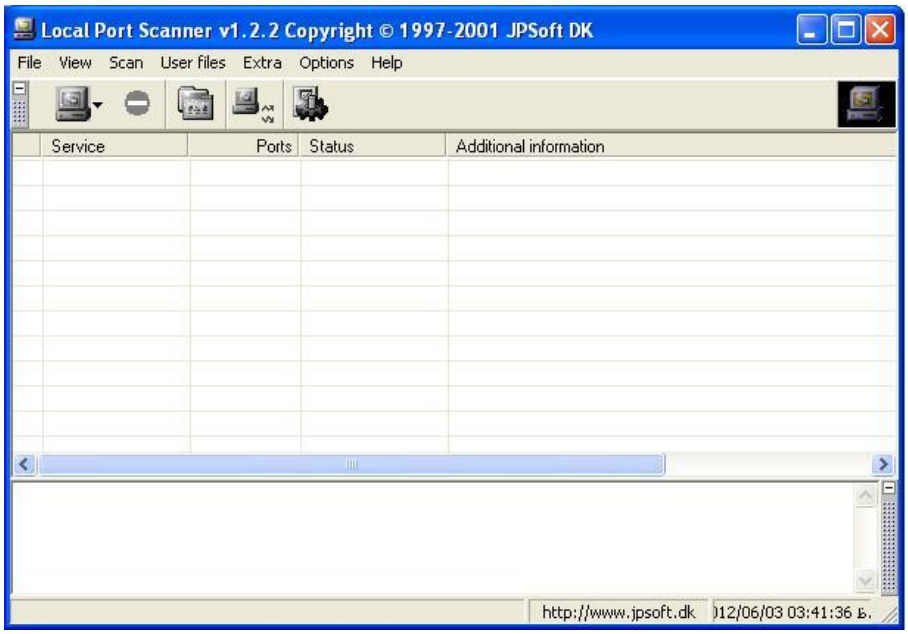
http://www.t1shopper.com/tools/port-scan/

بعد از ورود به وب سایت بالا صفحه ی زیر را مشاهده می کنید



در قسمت Home name or IPV4 address شما می توانید ایپی کامپیوتر خودتان را به آن دهید که برای بدست آوردن آدرس ایپی خود به سایت WWw.MyIpAddress.com مراجعه نمایید .و در قسمت های دیگر می توانید یک رنج خاص از پرت ها را انتخاب کنید و یا چند پرت خاص را فقط بنویسید و یا نه در میان پورت هایی که خود سایت معرفی کرده عملیات جستجو را انجام دهید . بر روی Scan کلیک کنید و نتیجه را ببینید .(کمتر از ۱ ثانیه به شما پاسخ می دهد)

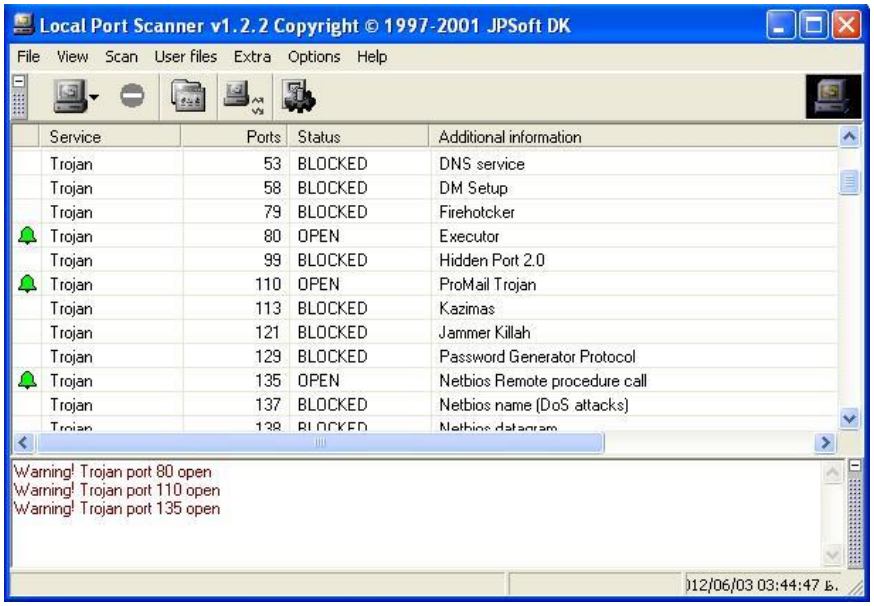




بر نامه ی بالا دارای حالت های مختلف برای اسکن کردن رنج پرت ها می باشد

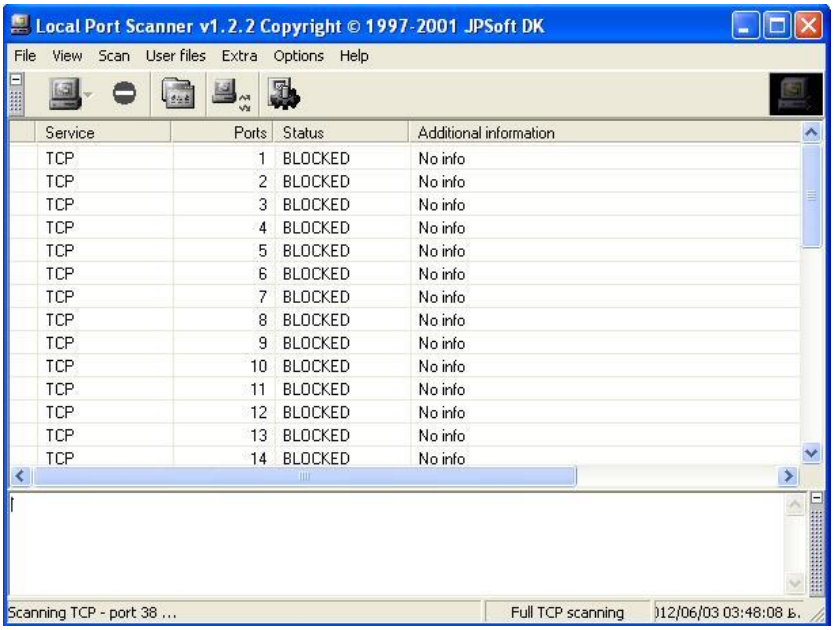
با کلیک روی منوی Scan و یا شکل کامپیوتر (Start Scan) می توانید نوع های آن را مشاهده نمایید .

Trojan Scan : که دارای یک پایگاه داده می باشد که در آن لیستی از تمامی پورت هایی که تروجان های مختلف از آن استفاده کرده اند را دارا می باشد . DB را می توانید در منوی User File مشاهده نمایید



برنامه لیستی از پورت ها را برای ما می آورد و وضعیت آن را به ما می گوید به عنوان مثال در این سیستم پورتهای , 80 137 , 110 باز می باشد .

همچنین می توان با استفاده از گزینه ی Full Tcp Scan به اسکن تمامی پورت ها از ۱ تا ۶۵۵۳۵ بپردازید .

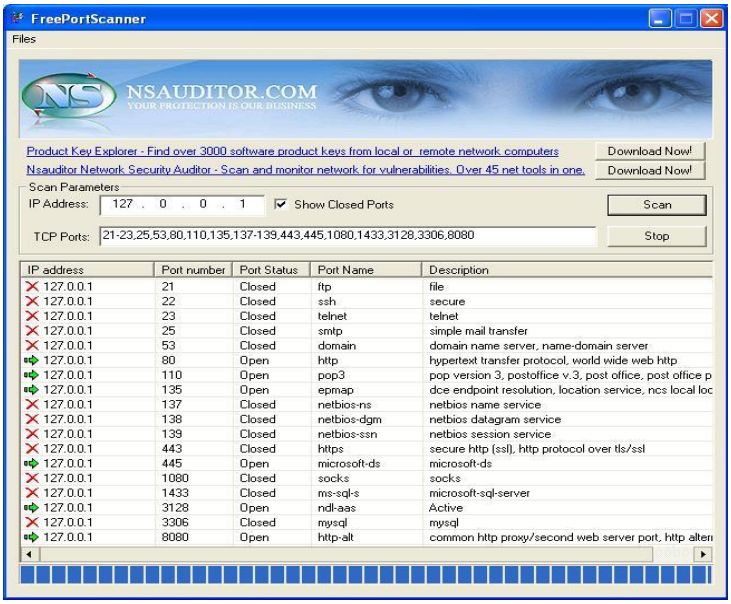


در صورتی که می خواهید چند پورت خاص را فقط اسکن نمایید می توانید از طریق منوی User File گزینه ی User.lpsرا انتخاب نمایید و سپس پورت هایی که می خواهید اسکن شود را در آن وارد کنید و سپس از منوی Scan بر روی گزینه ی User DefindScan کلیک نمایید .

بهترین اسکن هم در این ابزار گزینه ی Quick Scan می باشد که در آن تمامی پورت های معروف و کاربردی اسکن می شود

FreePortScanner

این نرم افزار یکی دیگر از بهترین نرم افزار های پویش پورت بر روی سیستم شما می باشد که سازنده ی آن وب سایت http://www.nsauditor.com/network_tools/free_port_scanner.html می باشد که در آن نرم افزار های متنوعی وجود دارد که البته این نرم افزار به صورت رایگان عرضه شده



کافیست که در قسمت ip address ایپی محلی خود که ۱۲۷.۰.۰.۱ را بزنید و در قسمت TCPport هم پورت هایی که می خواهید آن را پویش نمایید را وارد کنید .

دیگر نرم افزار هایی که در این ضمینه وجود دارد می توان Netcat – nmap – local port scanner را نام برد .

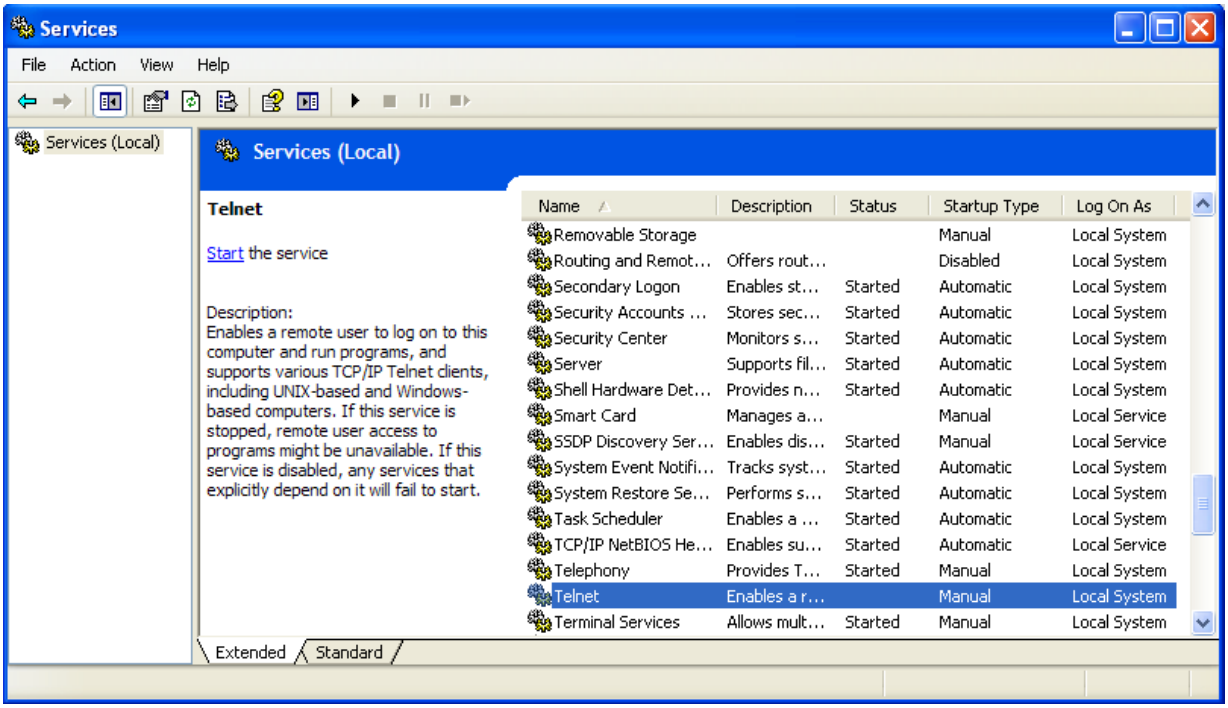
بستن پورت ها بر روی ویندوز

- **با استفاده از بستن سرویس ها**

سرویس های ویندوز اولین برنامه هایی هستند که در هنگام بالا آمدن ویندوز اجرا می شوند و به منظور ارائه ی سرویس خاصی ایجاد شده اند که دارای سطح دسترسی بالاتر از Administrator هستند. (یعنی سطح دسترسیsystem) این سرویس ها ممکن است جهت آغاز به کار به یک پورت باز نیاز داشته باشند و از پورت های **۰ تا ۱۰۲۳** که پورت های رزرو سیستم عامل می باشد یک پورت را که توسط برنامه نویس به آن اختصاص داده شده را باز کند . اگر بخواهیم پورت های که توسط سرویس ها باز شده است را ببندیم بهتر است سرویس آن رارغیر فعال کنیم . در زیر به ذکر چند روش آن می پردازیم

- **با استفاده از کنسول Services.msc**

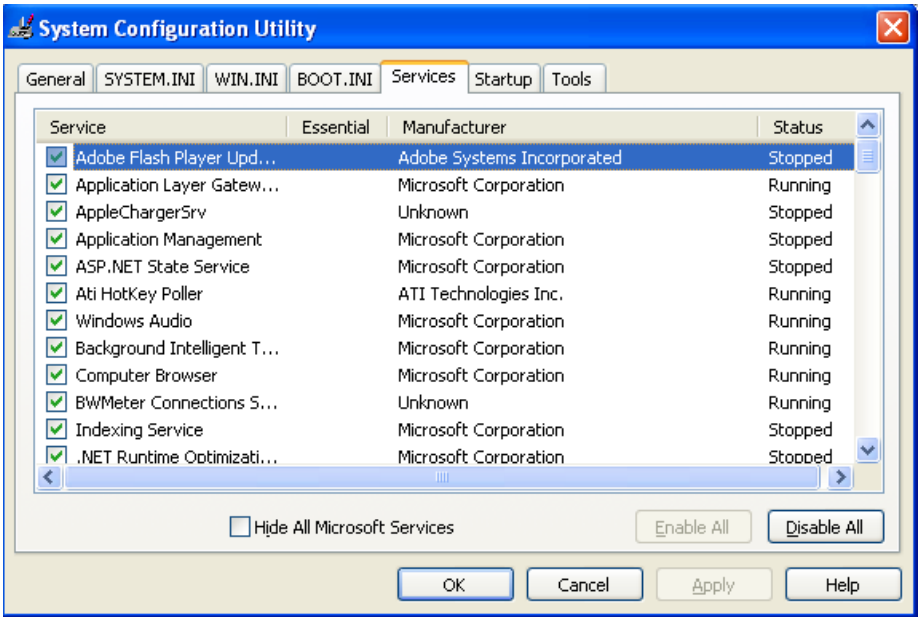
با استفاده از این برنامه می توانید لیستی از تمامی پورت ها را مشاهده کنید و روی آنها مدیریت کامل داشته باشید . برای ورود به این کنسول می توانید با نوشتن عبارت Services.msc در Run وارد آن شد و یا در Computer Managment بر روی آن کلیک نماییم و یا با استفاده از Control Panel گزینه ی Administrative Tools آن را انتخاب نمود .



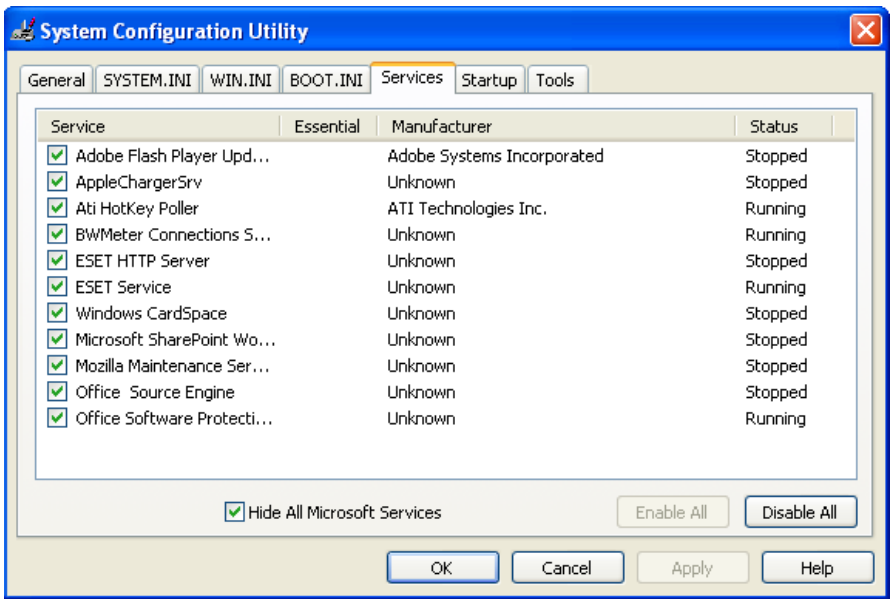
جهت مدیریت آنها کافیست بر روی یکی از سرویس ها کلیک راست نمایید .

با استفاده از System Configuration Utility

این برنامه هم یکی دیگر از برنامه های مفید در ویندوز می باشد که یکی از امکانات آن کار با سرویس های ویندوز می باشد و به شما امکان مدیریت بر روی سرویس ها را می دهد .



با تیکدار کردن گزینه ی Hide All Microsoft Services تمامی سرویس های پیش فرض سیستم عامل پنهان می شوند و فقط سرویس برنامه هایی که توسط شما بر روی سیستم عامل نصب شده است را نمایش می دهد .



با استفاده از فرامین ویندوز

Net Command

این سری فرامین هم می توانند به شما امکان می ریت در حد مبتدی را بدهند

net start *ServiceName*	این فرمان جهت راه اندازی یک سرویس به کار می رود
net stop *ServiceName*	این فرمان جهت متوقف کردن کامل یک سرویس به کار می رود
net pause *ServiceName*	این فرمان جهت متوقف کردن موقت یک سرویس به کار می رود
net continue *ServiceName*	این فرمان جهت اجرای دوباره سرویس Pause شده به کار می رود

کافیت به جای Service نام سرویس مورد نظر را بزنیم .

شما می توانید جهت نمایش service های فعال از فرمان Net start استفاده نمایید .

فرمان SC

این فرمان یکی از فرامین مورد علاقه ی برنامه نویس ها و مدیران امنیتی می باشد .که سویچ های فراوانی را دارد که ما اینجا فقط فرامین مورد نیاز را شرح می دهیم

SC Stop *ServiceName*	این فرمان جهت راه اندازی یک سرویس به کار می رود
SC Stop *ServiceName*	این فرمان جهت متوقف کردن کامل یک سرویس به کار می رود
sc pause *ServiceName*	این فرمان جهت متوقف کردن موقت یک سرویس به کار می رود
sc continue *ServiceName*	این فرمان جهت اجرای دوباره سرویس Pause شده به کار می رود
sc delete *ServiceName*	این فرمان جهت حذف کردن یک سرویس به کار می رود
SC Query	برای بدست آورد لیست سرویس ها همراه مشخصات کاملی از آنها

برای دریافت اطلاعات بیشتر در مورد این برنامه به لینک http://support.microsoft.com/kb/251192 مراجعه نمایید.

Indicates that the client just received acknowledgment of the first FIN signal from the server

متوقف کردن سرویس ها در رجیستری جهت مسدود شدن پورت آنها

مسدود کردن پورت ۱۳۵

به مسیر زیر در رجیستری بروید

HKEY_LOCAL_MACHINE\Software\Microsoft\OLE

سپس مقدار EnableDCOM را به "N" تغییر دهید .

دوباره به مسیر زیر رفته

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RPC

و مقدار DCOM Protocols را حذف نمایید .

مسدود کردن پورت ۴۴۵

به مسیر زیر از رجیستری بروید

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

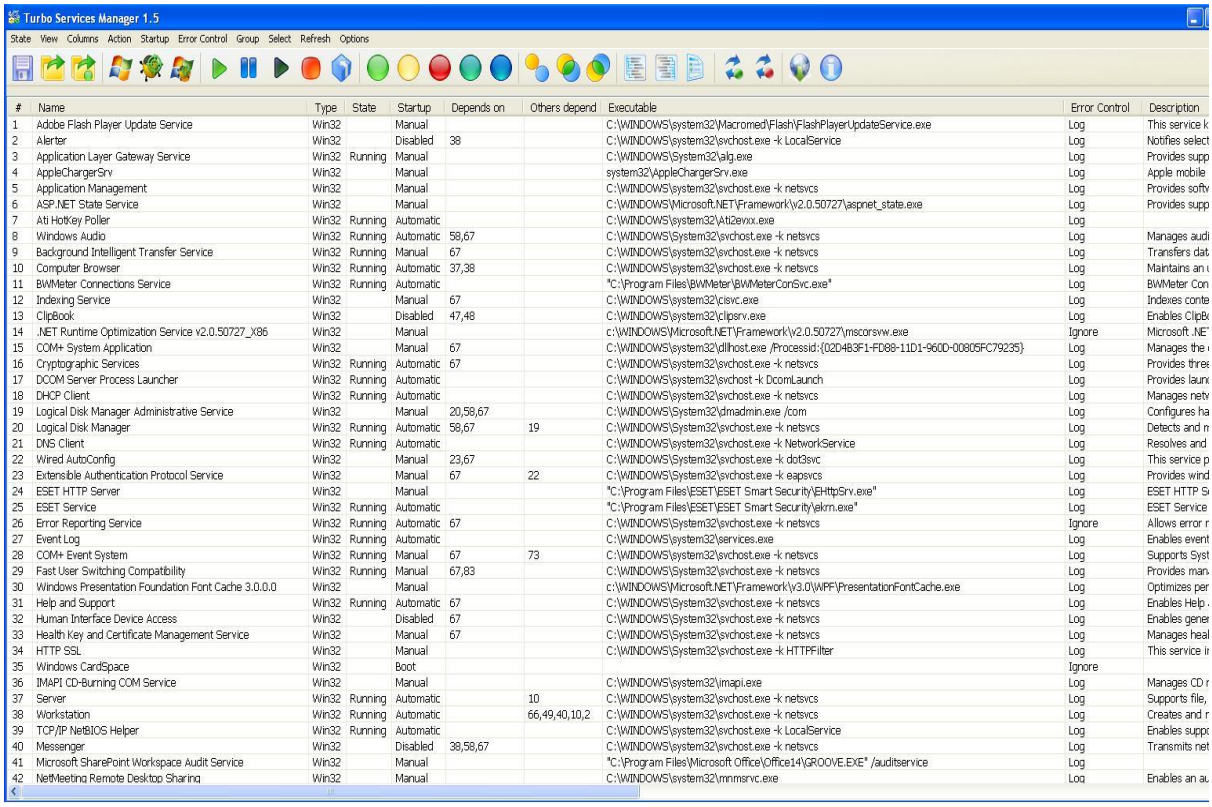
مقدار SMBDeviceEnabled را به ۰ تغییر دهید .

جهت کسب اطلاعات بیشتر در ضمینه ی کار با رجیستری و دیگر روش ها در یان ضمینه می توانید به کتاب زیر مراجعه نمایید . کتاب به صورت رایگان نیست اما با سرچ ساده ای در گوگل هزاران نسخه ی رایگان آن برای دانلود گذاشته شده است .خواندن این کتاب خالی از لطف نیست .

Microsoft® Windows® XP Registry Guide

استفاده از ابزار Turbo Service Manager

این ابزار هم حالت گرافیکی فرامین بالا می باشد که دارای امکاناتی فوق العاده در ضمینه ی کنترل سرویس های ویندوزی می باشد .



#	Name	Type	State	Startup	Depends on	Others depend	Executable	Error Control	Description
1	Adobe Flash Player Update Service	Win32		Manual			C:\WINDOWS\system32\Macromed\Flash\FlashPlayerUpdateService.exe	Log	This service k
2	Alerter	Win32		Disabled	38		C:\WINDOWS\system32\svchost.exe -k LocalService	Log	Notifies select
3	Application Layer Gateway Service	Win32	Running	Manual			C:\WINDOWS\System32\alg.exe	Log	Provides supp
4	AppleChargerSrv	Win32		Manual			system32\AppleChargerSrv.exe	Log	Apple mobile
5	Application Management	Win32		Manual			C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Provides softv
6	ASP.NET State Service	Win32		Manual			C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe	Log	Provides supp
7	Ati HotKey Poller	Win32	Running	Automatic			C:\WINDOWS\system32\ati2evxx.exe	Log	
8	Windows Audio	Win32	Running	Automatic	58,67		C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Manages audi
9	Background Intelligent Transfer Service	Win32	Running	Manual	67		C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Transfers dat
10	Computer Browser	Win32	Running	Automatic	37,38		C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Maintains an
11	BWMeter Connections Service	Win32	Running	Automatic			"C:\Program Files\BWMeter\BWMeterConSvc.exe"	Log	BWMeter Con
12	Indexing Service	Win32		Manual	67		C:\WINDOWS\system32\cisvc.exe	Log	Indexes conte
13	ClipBook	Win32		Disabled	47,48		C:\WINDOWS\system32\clipsrv.exe	Log	Enables ClipB
14	.NET Runtime Optimization Service v2.0.50727_X86	Win32		Manual			c:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe	Ignore	Microsoft .NE
15	COM+ System Application	Win32		Manual	67		C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}	Log	Manages the
16	Cryptographic Services	Win32	Running	Automatic	67		C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Provides thre
17	DCOM Server Process Launcher	Win32	Running	Automatic			C:\WINDOWS\system32\svchost -k DcomLaunch	Log	Provides laun
18	DHCP Client	Win32	Running	Automatic			C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Manages netv
19	Logical Disk Manager Administrative Service	Win32		Manual	20,58,67		C:\WINDOWS\System32\dmadmin.exe /com	Log	Configures ha
20	Logical Disk Manager	Win32	Running	Automatic	58,67	19	C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Detects and
21	DNS Client	Win32	Running	Automatic			C:\WINDOWS\system32\svchost.exe -k NetworkService	Log	Resolves and
22	Wired AutoConfig	Win32		Manual	23,67		C:\WINDOWS\System32\svchost.exe -k dot3svc	Log	This service p
23	Extensible Authentication Protocol Service	Win32		Manual	67	22	C:\WINDOWS\System32\svchost.exe -k eapsvcs	Log	Provides wind
24	ESET HTTP Server	Win32		Manual			"C:\Program Files\ESET\ESET Smart Security\EHttpSrv.exe"	Log	ESET HTTP S
25	ESET Service	Win32	Running	Automatic			"C:\Program Files\ESET\ESET Smart Security\ekrn.exe"	Log	ESET Service
26	Error Reporting Service	Win32	Running	Automatic	67		C:\WINDOWS\System32\svchost.exe -k netsvcs	Ignore	Allows error
27	Event Log	Win32	Running	Automatic			C:\WINDOWS\system32\services.exe	Log	Enables event
28	COM+ Event System	Win32	Running	Manual	67	73	C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Supports Syst
29	Fast User Switching Compatibility	Win32	Running	Manual	67,83		C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Provides man
30	Windows Presentation Foundation Font Cache 3.0.0.0	Win32		Manual			c:\WINDOWS\Microsoft.NET\Framework\v3.0\WPF\PresentationFontCache.exe	Log	Optimizes per
31	Help and Support	Win32	Running	Automatic	67		C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Enables Help
32	Human Interface Device Access	Win32		Disabled	67		C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Enables gener
33	Health Key and Certificate Management Service	Win32		Manual	67		C:\WINDOWS\System32\svchost.exe -k netsvcs	Log	Manages heal
34	HTTP SSL	Win32		Manual			C:\WINDOWS\System32\svchost.exe -k HTTPFilter	Log	This service i
35	Windows CardSpace	Win32		Boot				Ignore	
36	IMAPI CD-Burning COM Service	Win32		Manual			C:\WINDOWS\system32\imapi.exe	Log	Manages CD
37	Server	Win32	Running	Automatic		10	C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Supports file,
38	Workstation	Win32	Running	Automatic		66,49,40,10,2	C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Creates and
39	TCP/IP NetBIOS Helper	Win32	Running	Automatic			C:\WINDOWS\system32\svchost.exe -k LocalService	Log	Enables suppo
40	Messenger	Win32		Disabled	38,58,67		C:\WINDOWS\system32\svchost.exe -k netsvcs	Log	Transmits net
41	Microsoft SharePoint Workspace Audit Service	Win32		Manual			"C:\Program Files\Microsoft Office\Office14\GROOVE.EXE" /auditservice	Log	
42	NetMeeting Remote Desktop Sharing	Win32		Manual			C:\WINDOWS\system32\mnmsrvc.exe	Log	Enables an au

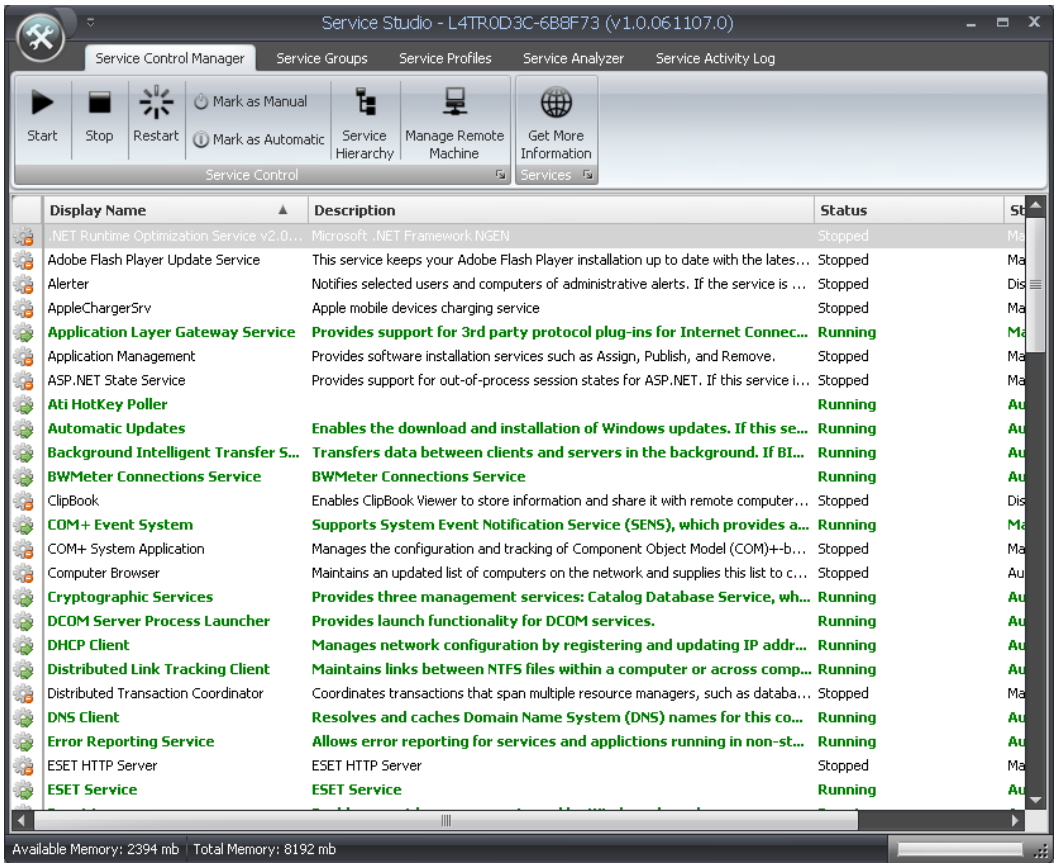
همان طور که میبینید این نرم افزار دارای قدرتی فراوان در ضمینه ی مدیریت سرویس های ویندوز می باشد .

برای دانلود به لینک زیر مراجعه نمایید

http://www.turboirc.com/link.php?x=1201

با استفاده از ابزار Service Studio

یکی دیگر از ابزار های قوی جهت آنالیز و کار با سرویس های ویندوز برنامه ی Service Studio می باشد که دارای قدرت فراوانی در مدیریت می باشد .



برای دانلود می توانید از لینک زیر استفاده کنید

http://mindswarm.com/Releases/ServiceStudio_v1.zip

کار با پورت ها با استفاده از فایروال ویندوز

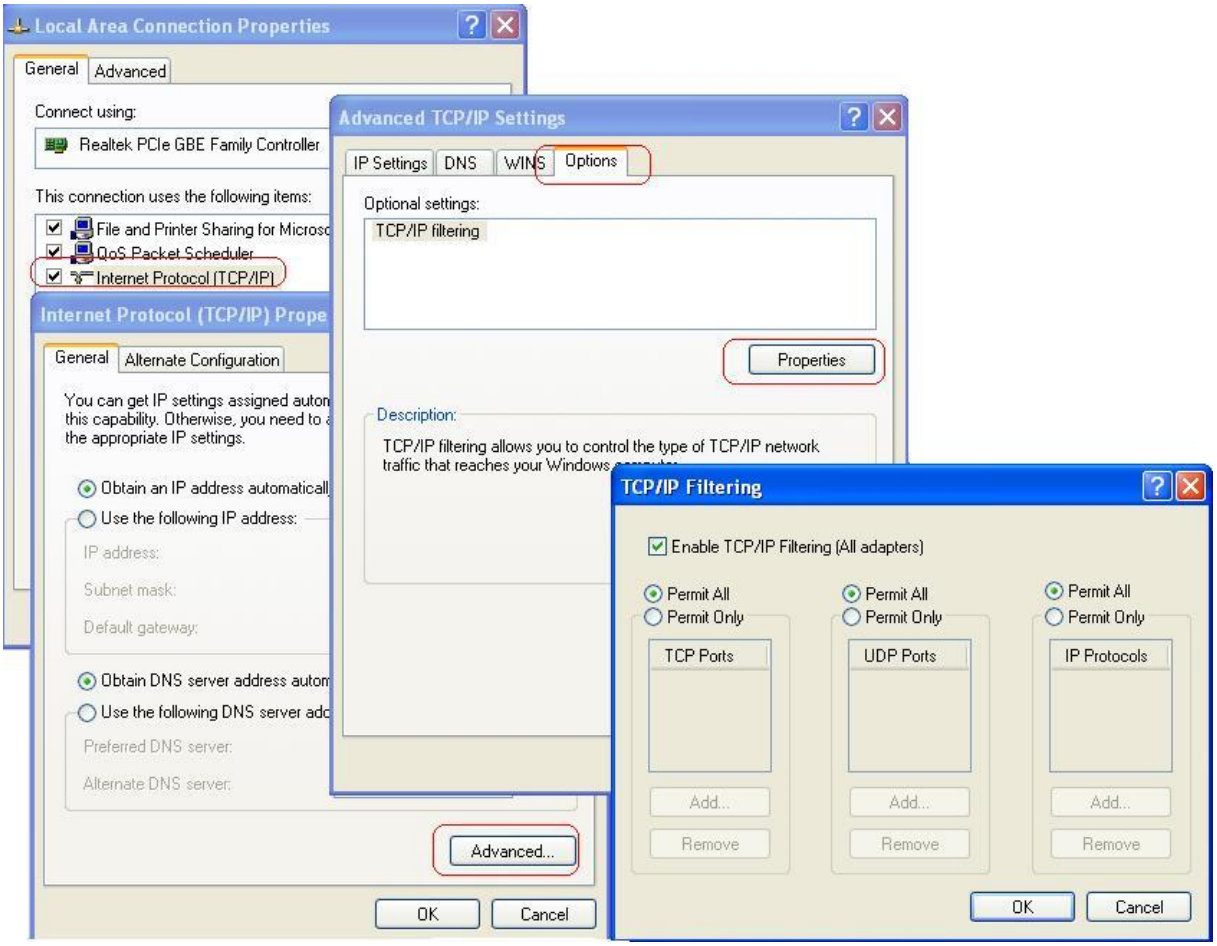
یکی از مهمترین وظایف فایروال در سیستم عامل مدیریت پورت ها می باشد یعنی بسیار راحت می توان پورتی را باز یا فیلتر و یا مسدود کرد و یا برنامه ای که باعث باز شدن پورتی خاص در سیستم شما می شود را فیلتر کنید و به آن اجازه ی انجام این کار ندهید .این کار در فایروال به دو روش انجام می شود

- با استفاده از برنامه Windows Firewal

یکی از امکانات فایروال ویندوز امکان فیلتر کردن پورت ها می باشد یعنی می توان مشخص کرد که کدام پورت های UDB یا TCP می تواند مورد استفاده قرار گیرد .برای انجام این کار مراحل زیر را طی می نماییم .

Control panel >> Netw0rk connetion >> Local Area Connection >> General >> internet Protocol (TCP/Ip) Advance >> Option >> TCP/IP Filtering

با انجام موارد بالا پنجره ی زیر ظاهر می شود .

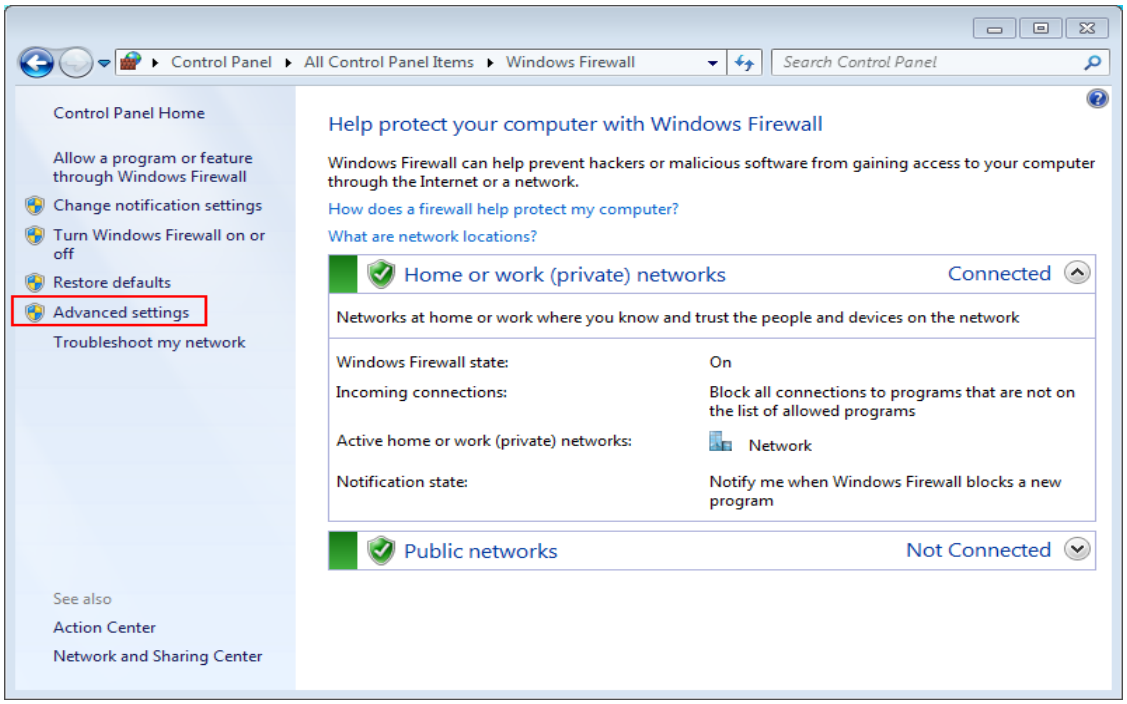


خوب در اینجا می توانید هم UDP Port, TCP Port, IP Protocols ها را فیلتر کرد فقط کافیست برروی Premit Only کلیک نمایید و لیست پورت هایی که می خواهید روی سیستم شما بتواند مورد استفاده قرار گیرد را به لیست اضافه کنید

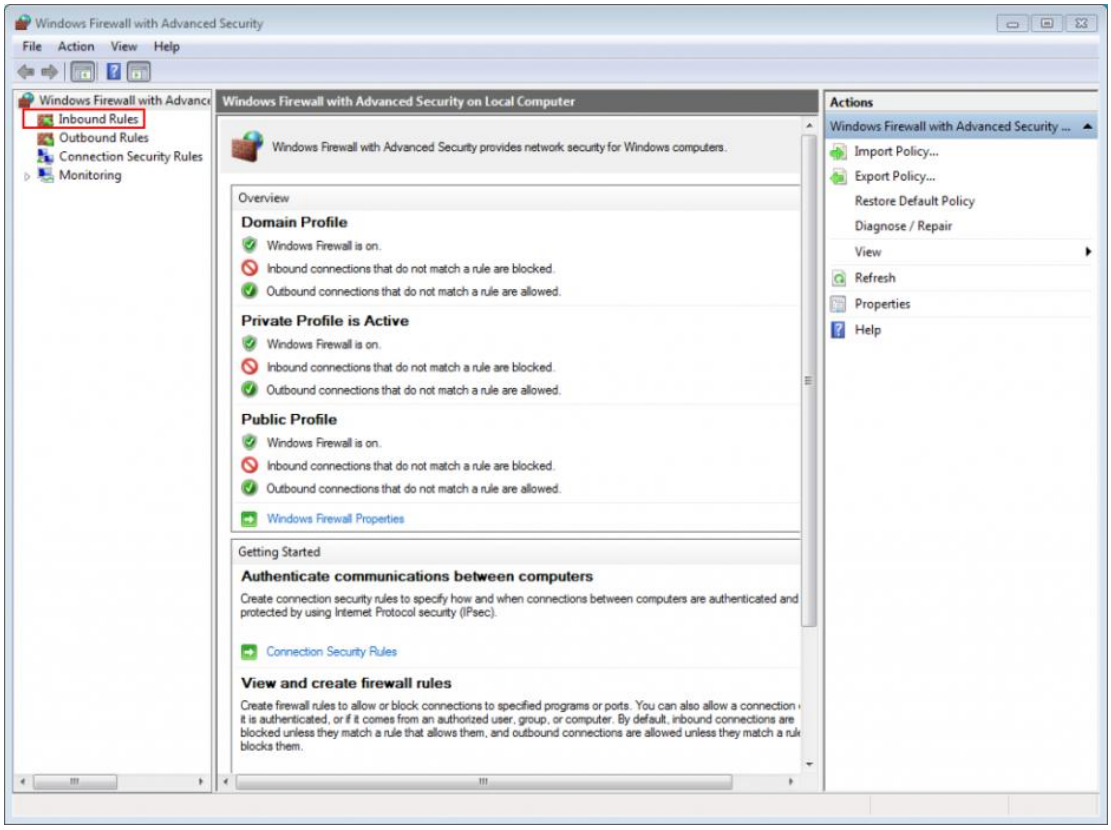
نکته : اگر Permit Only را انتخاب کنید و هیچ گزینه ای را به آن اضافه کنید به این معنی بوده که هیچ پورتی بر روی سیستم نمی تواند مورد استفاده قرار گیرد .

اما در ویندوز Seven وضعیت فرق می کند و نحوه ی بستن پورت ها با روش متفاوتی صورت می گیرد که آن را شرح می دهیم

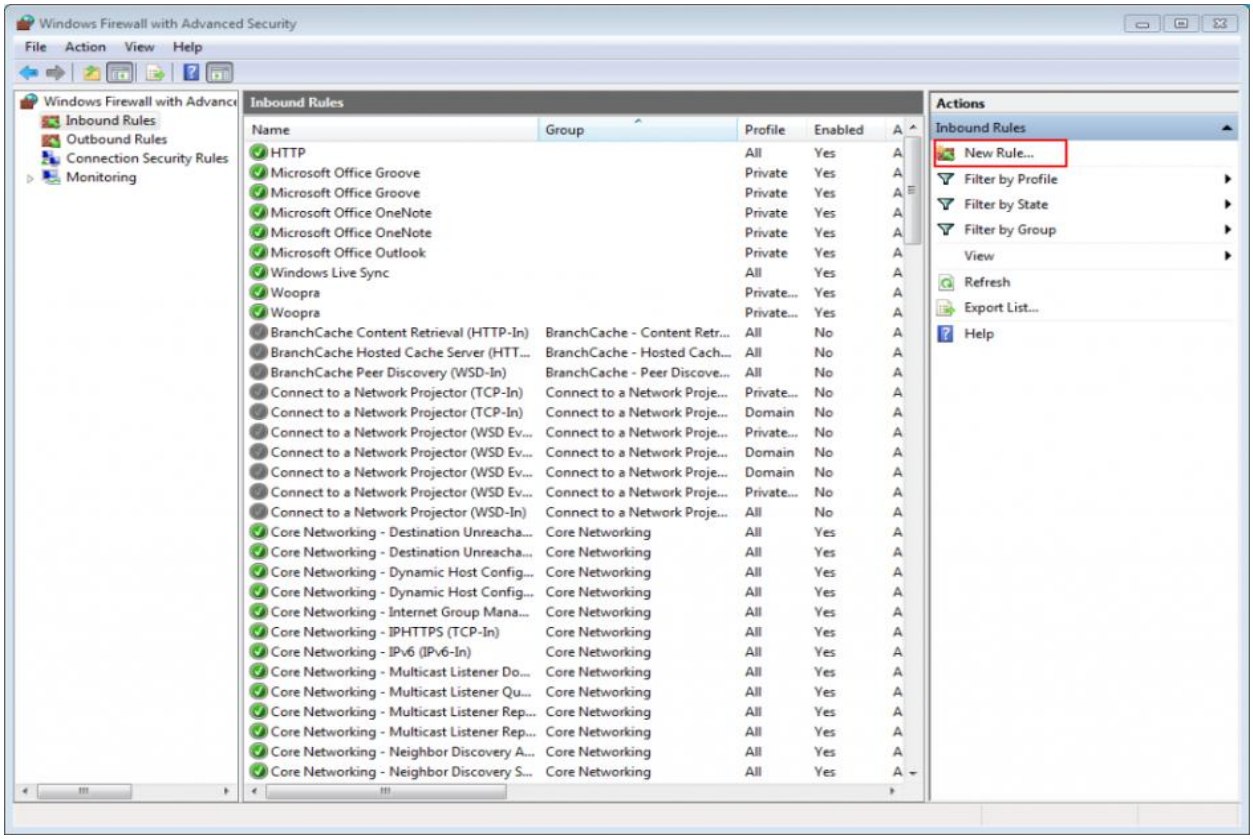
به کنترل پانل ویندوز بروید و گزینه ی Windows Firewall را انتخاب نمایید .



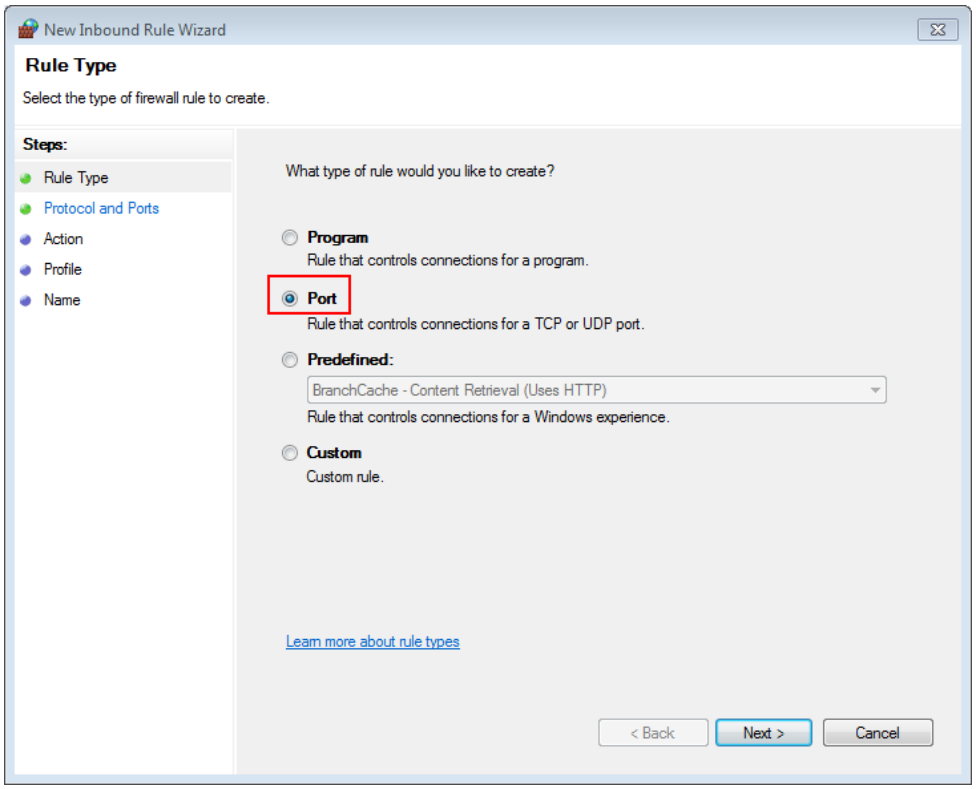
در پنجره ی باز شده بر روی Advanced Settings کلیک نمایید .تا پنجره ی زیر ظاهر شود



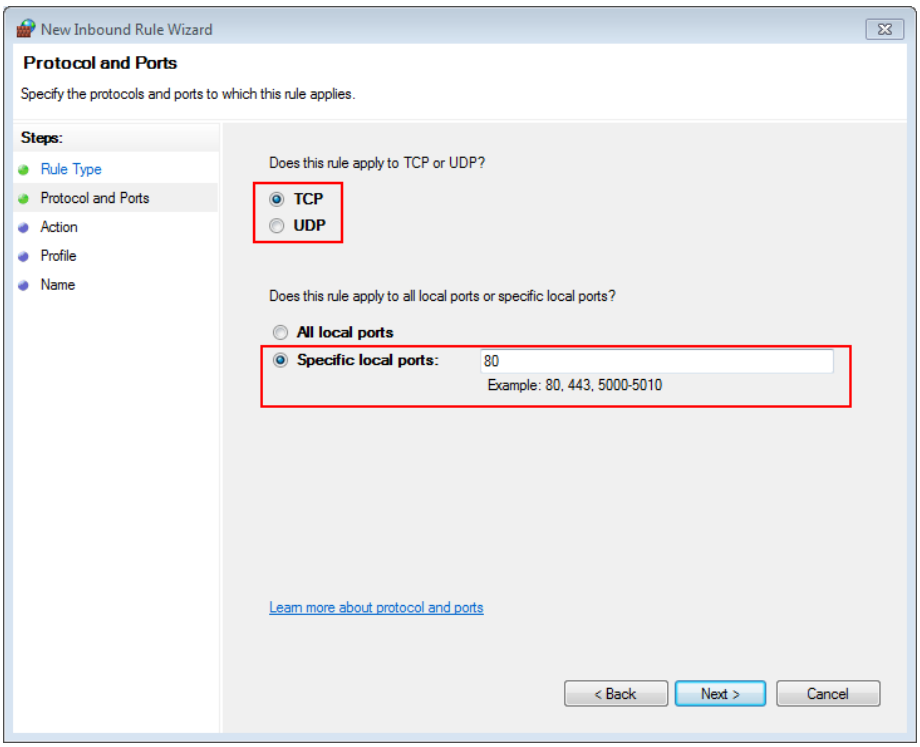
در این پنجره بر روی **Inbound Rules** کلیک نمایید



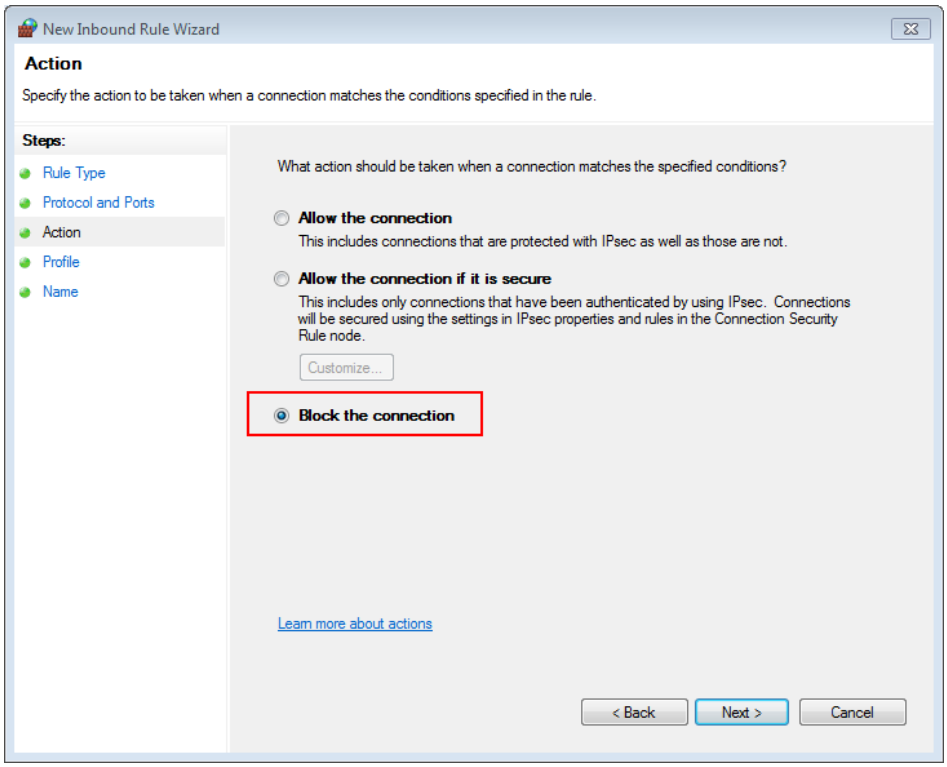
سپس بر روی New Role کلیک نمایید



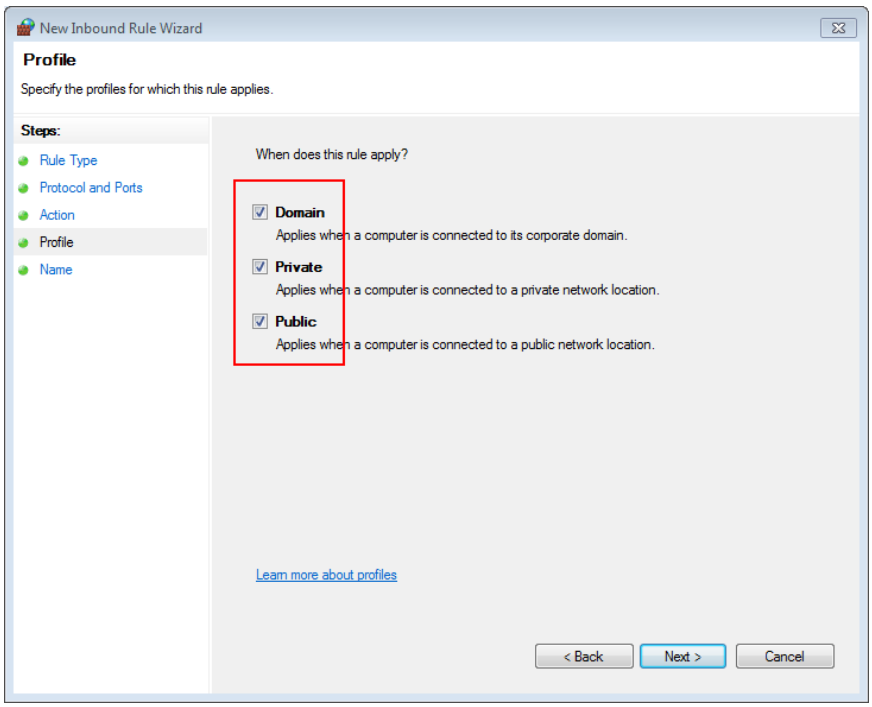
در ادامه بر روی Port کلیک نمایید .



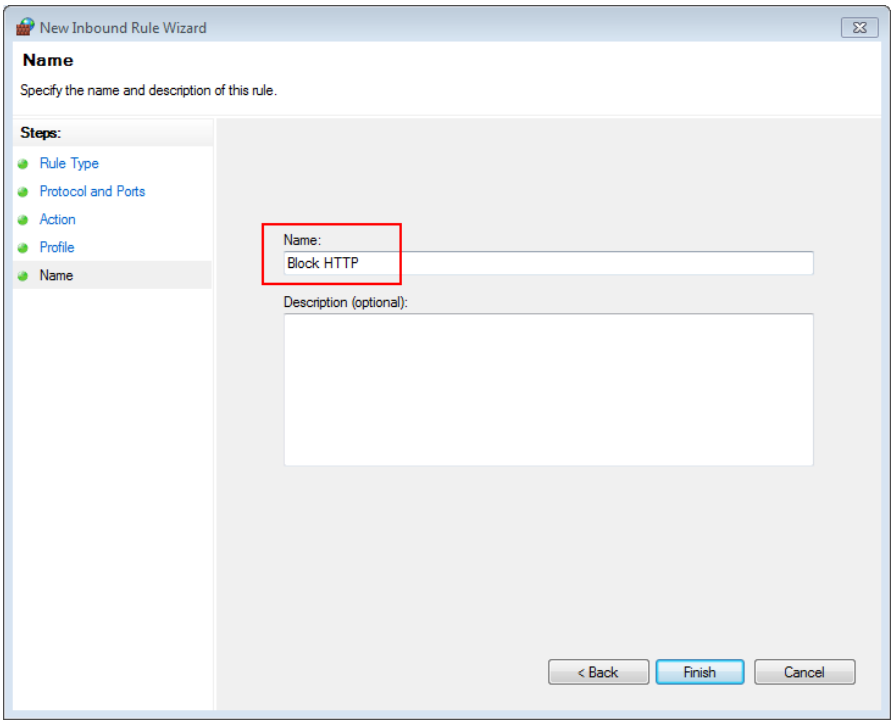
در این قسمت باید برروی Specifiv Local Ports کلیک نمایید و سپس در کادر مقابل آن پورت های 80,81,82 یا ۴۴۳ یا ازپورت های ۵۰۰۰تا ۲۰۱۰ استفاده نمایید بهتر است از پورت ۸۰ استفاده کنیم برای وارد کردن چند پورت می توانید از علامت کاما (,) استفاده نمایید .



در این قسمت بر روی گزینه ی Block The Connection کلیک نمایید .



در این قسمت هر ۳ گزینه را تیک دار کنید .



در نهایت نامی را برای Rule جدید که ایجاد کرده اید بنواسید و بر روی Finish کلیک نمایید .

بستن پورت ها با استفاده از فرمان Netsh

Netsh هم حالت تحت داس فایروال ویندوز می باشد که بیشتر مورد نیاز مدیران امنیتی می باشد این برنامه توانایی بسیار بالای در پیکر بندی فایروال را دارد .بااستفاده یکی از سویچ های آن ما می توانیم پورت های سیستم عامل رو مسدود و یا باز کنیم .

برای بستن یک پورت باز باید از فرمان زیر استفاده کنیم .

Netsh Firewall Delete

در زیر ۲ مثال را برای شما میزنیم

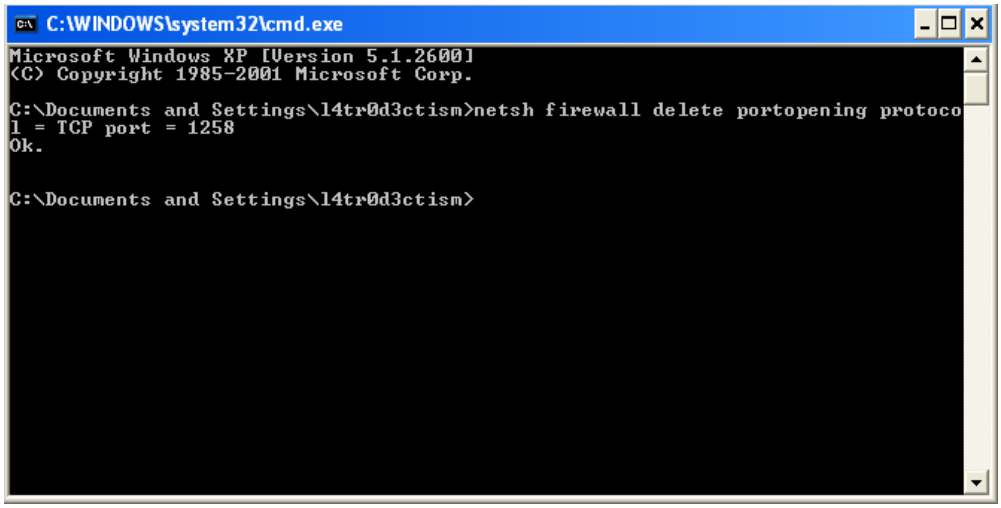
با استفاده از دستور زیر تمام rule ها را برای پورت ۸۰ حذف می کند

netsh firewall delete rule name=all protocol=tcp localport=80

و این فرمان هم برای بستن پورت ۴۴۵ می باشد

netsh firewall delete portopening protocol = TCP port = 1258

فقط کافیست جلوی Port شماره پورت مورد نظر را بنویسید تا آن پورت کامل بسته شود .



برای کسب اطلاعات بیشتر در مورد این فرمان و سویچ های مختلف آن به آدرس زیر بروید .

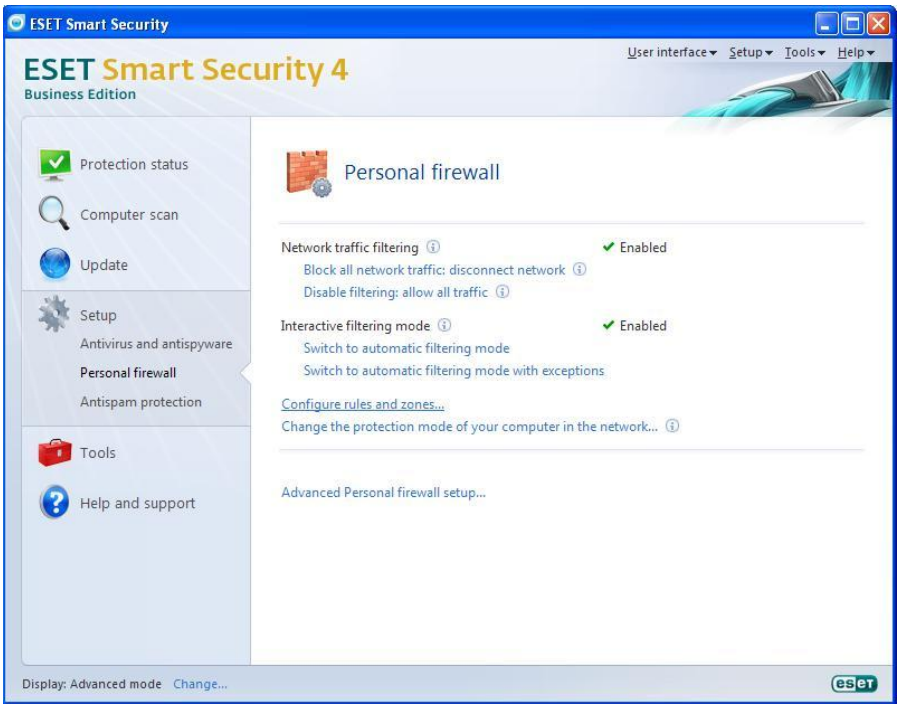
http://technet.microsoft.com/en-us/library/dd734783%28v=ws.10%29.aspx

مسدود کردن پورت ها از طریق فایروال های معروف

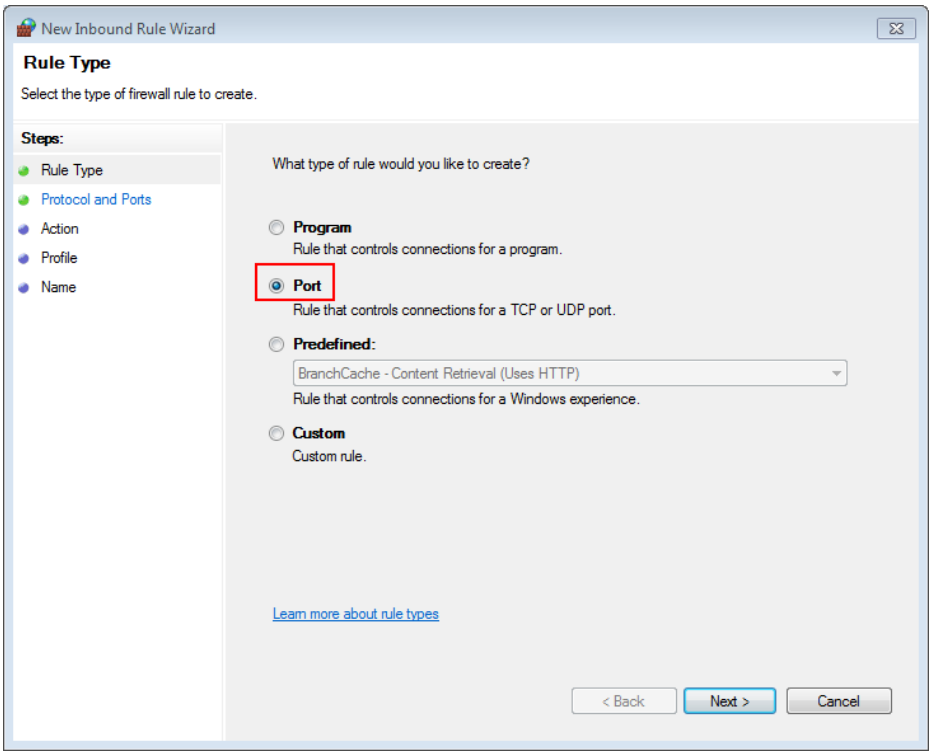
همیشه بهترین روش جهت بستن پورت کار با نرم افزار هایی هست که مستقیم برای این منظور نوشته شده است مثلا فایروال ها و Internet security های پر قدرت که توسط شرکت هایی که چندین متخصص واقعی را جهت برنامه نویسی آن دور خود جمع کرده است ساخته شده

نسخه ی Smart نود دارای یک فایروال بسیار ساده و البته قوی را ارا می باشد که در آن می توان Rule جدید را ایجاد نمایید و یا پورت خاصی را مسدود کنید .برای این کار به شکل زیر باید عمل کنید .

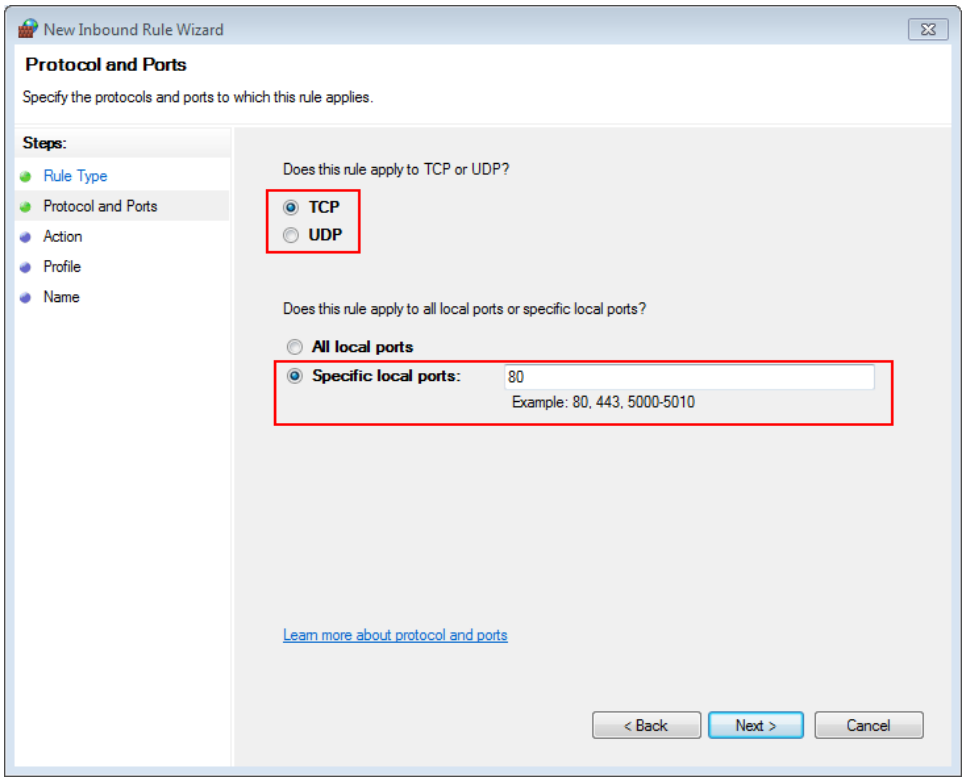
نرم افزار Nod32 Smart را باز کنید و به قسمت Setup بروید و Personal Firewall را انتخاب کنید سپس بر روی گزینه Configure Rule And Zones ... کلیک نمایید .



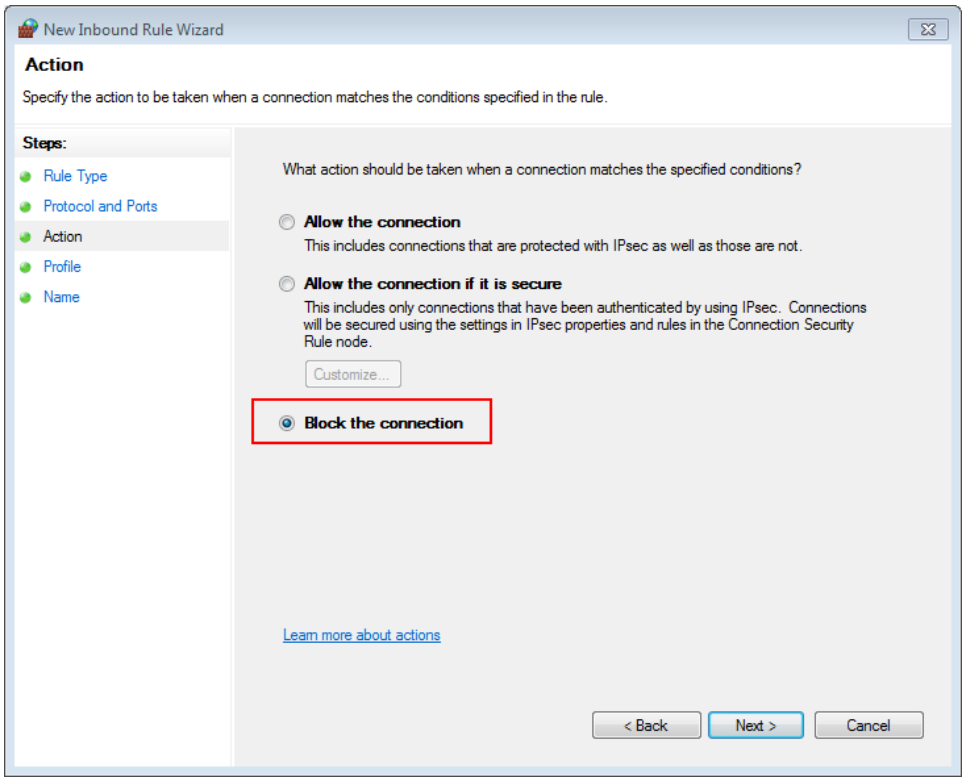
با انتخاب این گزینه ی گفته شده پنجره ی زیر ظاهر می شود که شما باید بر روی Port کلیک نمایید.



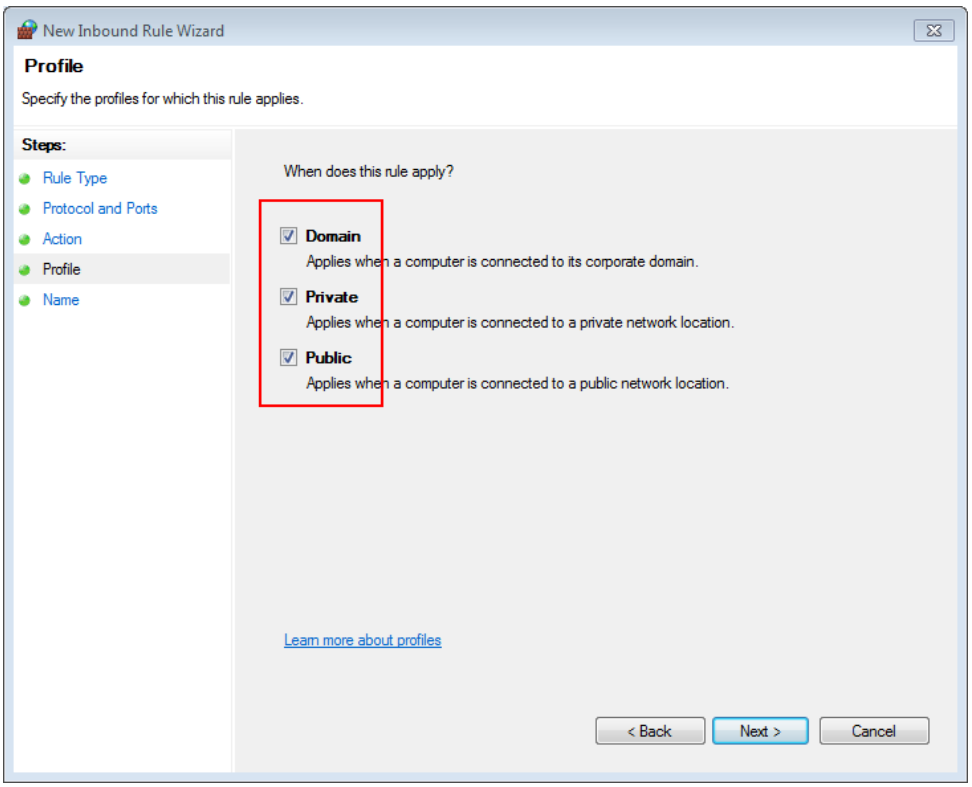
در مرحله ی بعد مشا می تاونید نوع پورت خود را انتخاب نمایید (UDP, TCP) و همچنین در قسمت زیرین آن یکی از پورت های 443 , 80 و یا ۵۰۰۰ تا ۵۰۱۰ را وارد کنید .



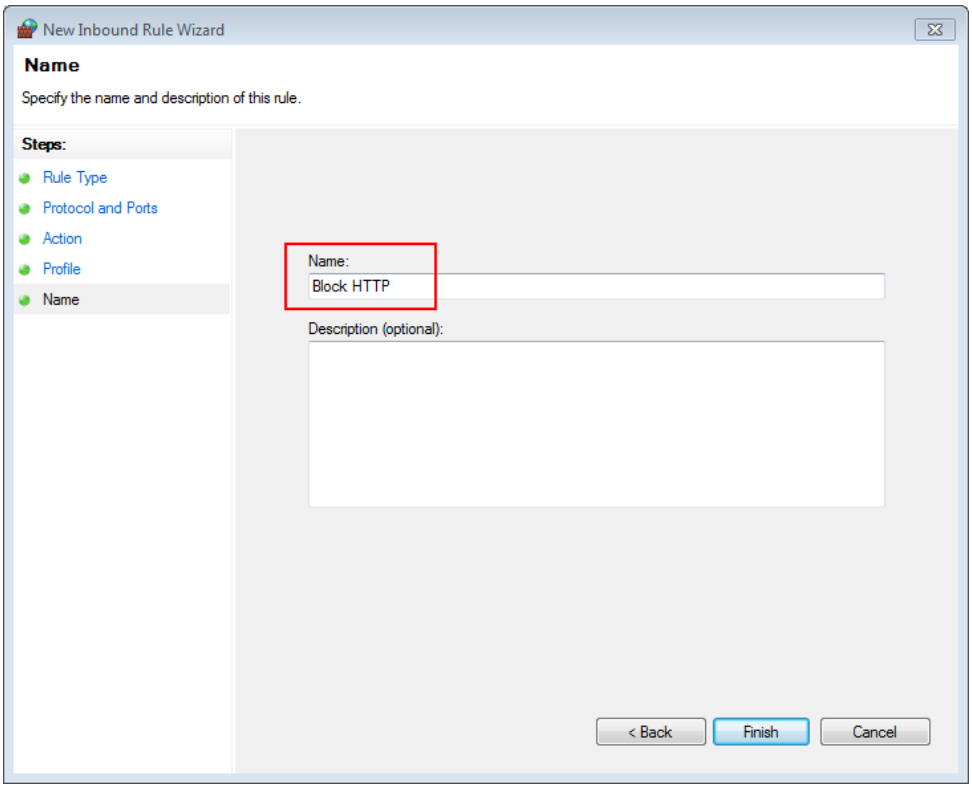
بر روی Block The Connection کلیک نمایید .



هر ۳ گزینه را تیک بزنید .



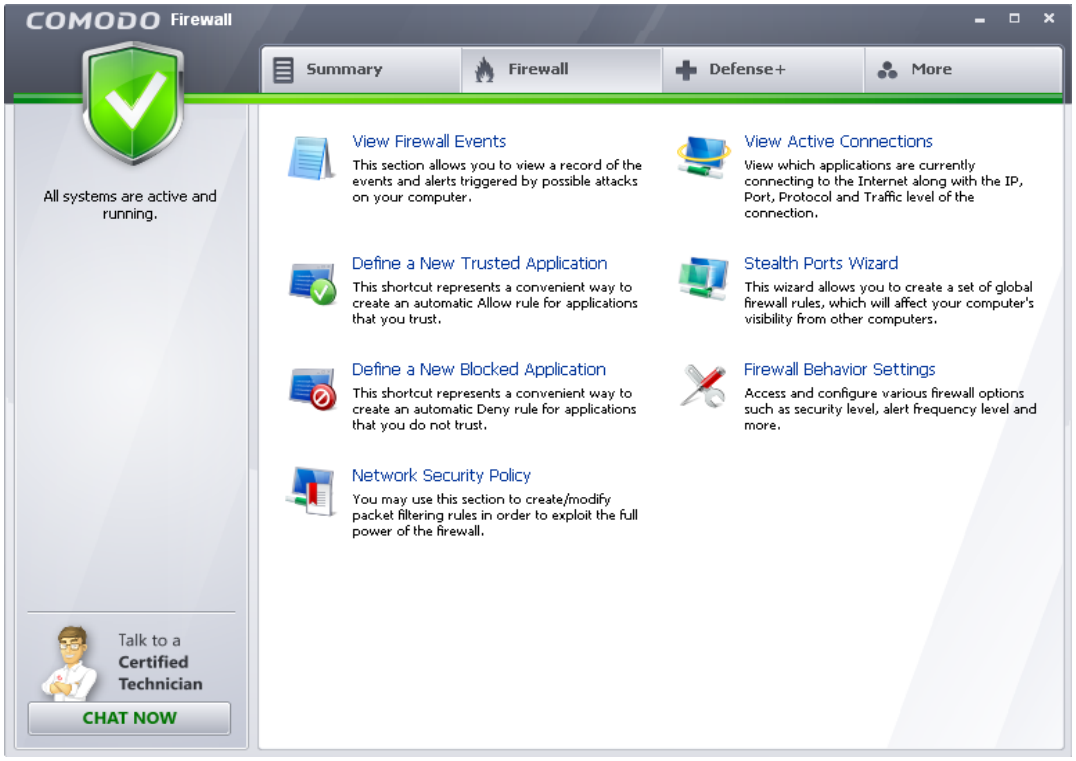
در نهایت با وارد کردن Name جهت ذخیره سازی Rule جدید تعریف شده پورت مشخص شده مسدود می شود .



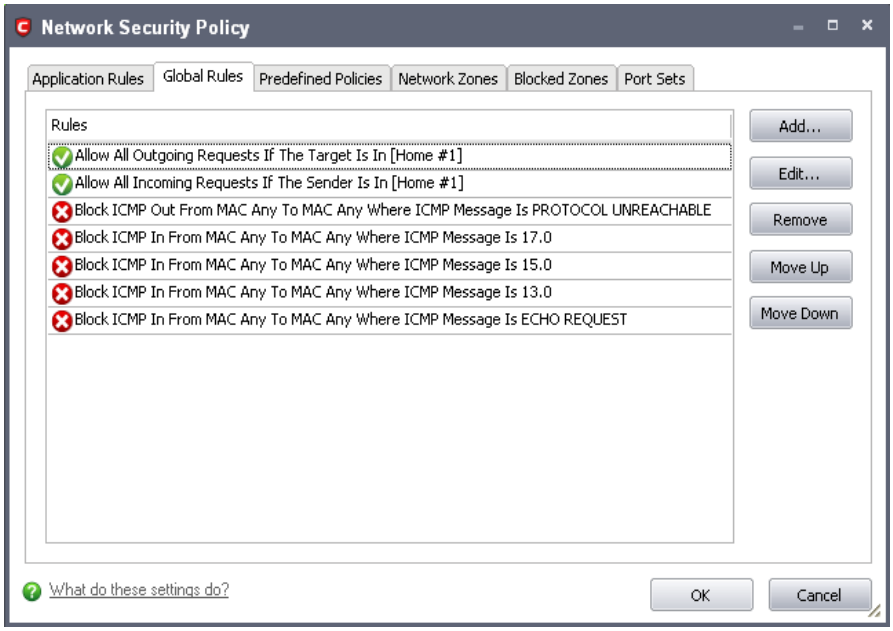
بستن پورت با استفاده از فایروال Comodo

کومودو در حال حاضر جزء بهترین فایروال هایی می باشد که برای ویندوز نوشته شده است این فایروال به صورت رایگان بوده و کار با آن بسیار ساده تر از ما بقیه ی فایروال ها می باشد در اینجا نحوه ی بستن پورت توسط این آنتی ویروس شرح می دهیم .

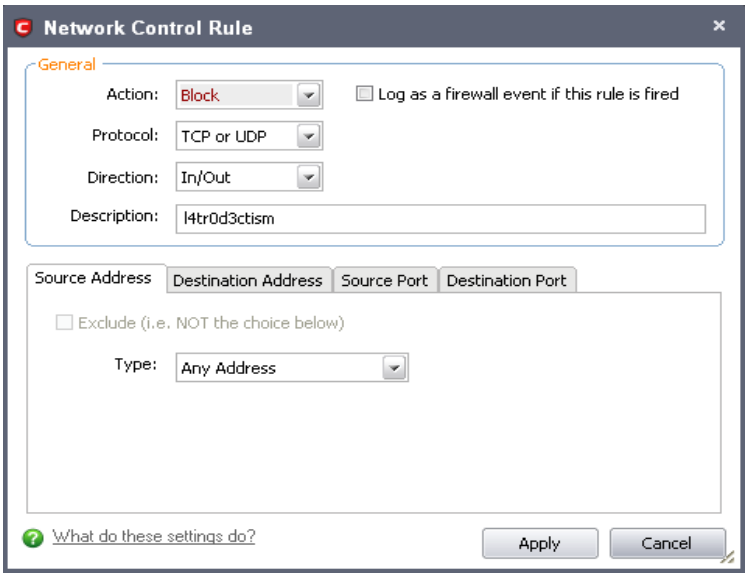
وارد صفحه ی اصلی برنامه شوید و بر روی سربرگ دوم آن یعنی Firewall کلیک نمایید



در این قسمت گزینه ی NetwOrk Security POlicy را انتخاب نمایید .



سپس در دومین سربرگ (Global Rules) بر روی Add کلیک نمایید



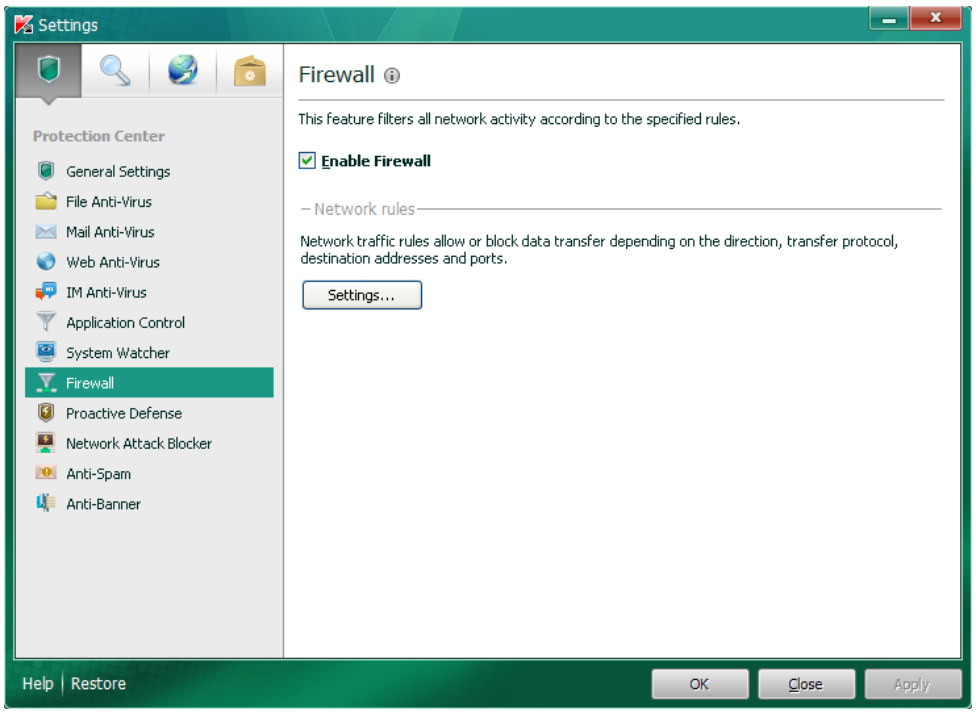
در این قسمت گزینه ی Block را جهت مسدود کردن پورت و گزینه ی open را جهت باز کردن پورت انتخاب کنید و در قسمت Protocol نوع پورت را انتخاب نمایید . و در نهایت بر روی Ok کلیک نمایید تا Rule مورد نظر به فایروال اضافه شود و در نهایت Apply را بزنید .

Kasper Sky Internet Security

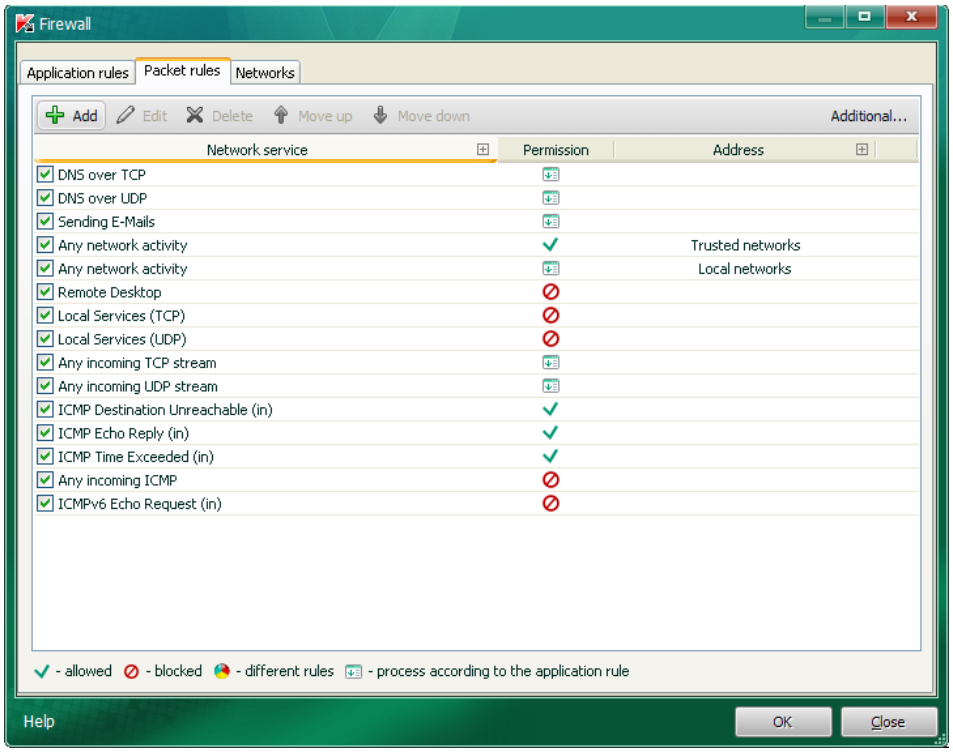
معروف ترین آنتی ویروس دنیا بوده در رده بندی های بهترین آنتی ویروس های دنیا معمولا در مقام ۱ تا ۳ قرار داره و با قدرت فراوان خود توجه حرفه ای ترین شرکت ها را به خود جلب کرده است . در این آنتی ویروس هم امکانات فراوانی برای کاربرا ن حرفه گذاشته شده است . جهت بستن پورت در این آنتی ویروس به شکل زیر عمل می کنیم .

بعد از باز کردن آنتی ویروس در صفحه ی اصلی بر روی گزینه Setting کلیک می نماییم

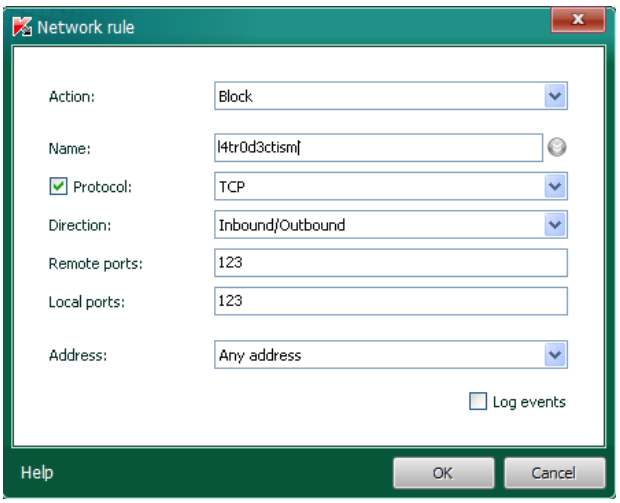
با کلیک روی این گزینه پنجره ی تنظیمات KasperSky ظاهر میشود .



در این پنجره هم Setting را در قسمت Firewall انتخاب می نماییم .



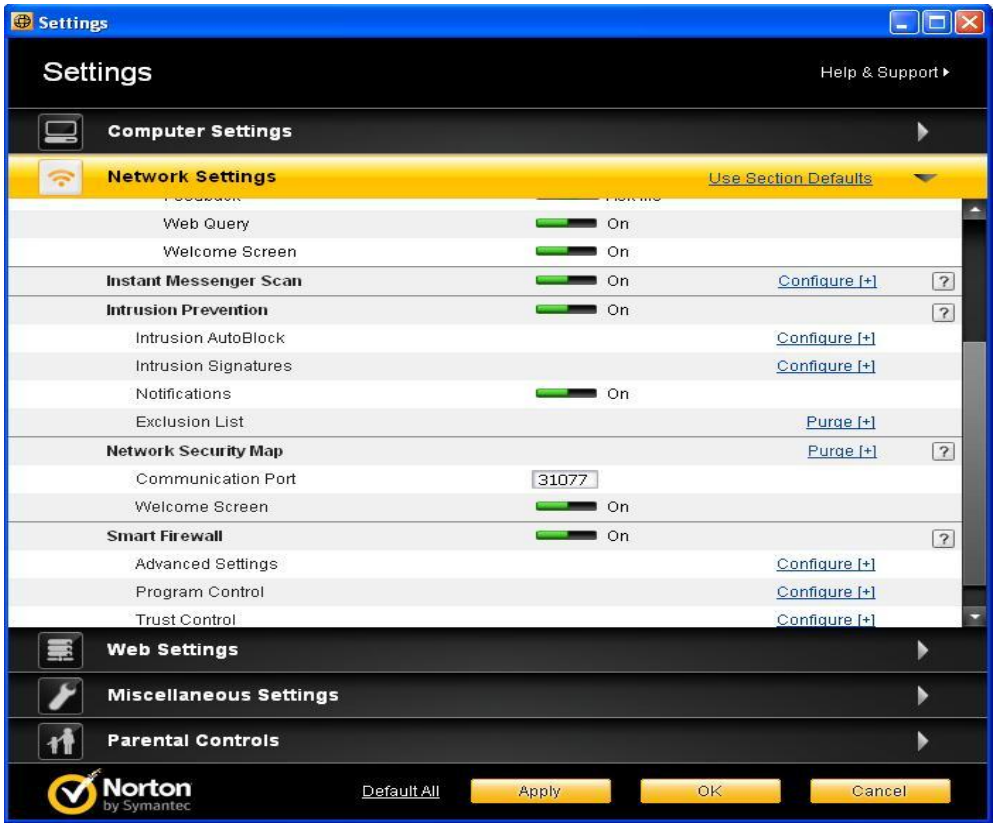
سپس بر روی دومین سربرگ Pocket Rules بر روی گزینه ی Add کلیک می نماییم .



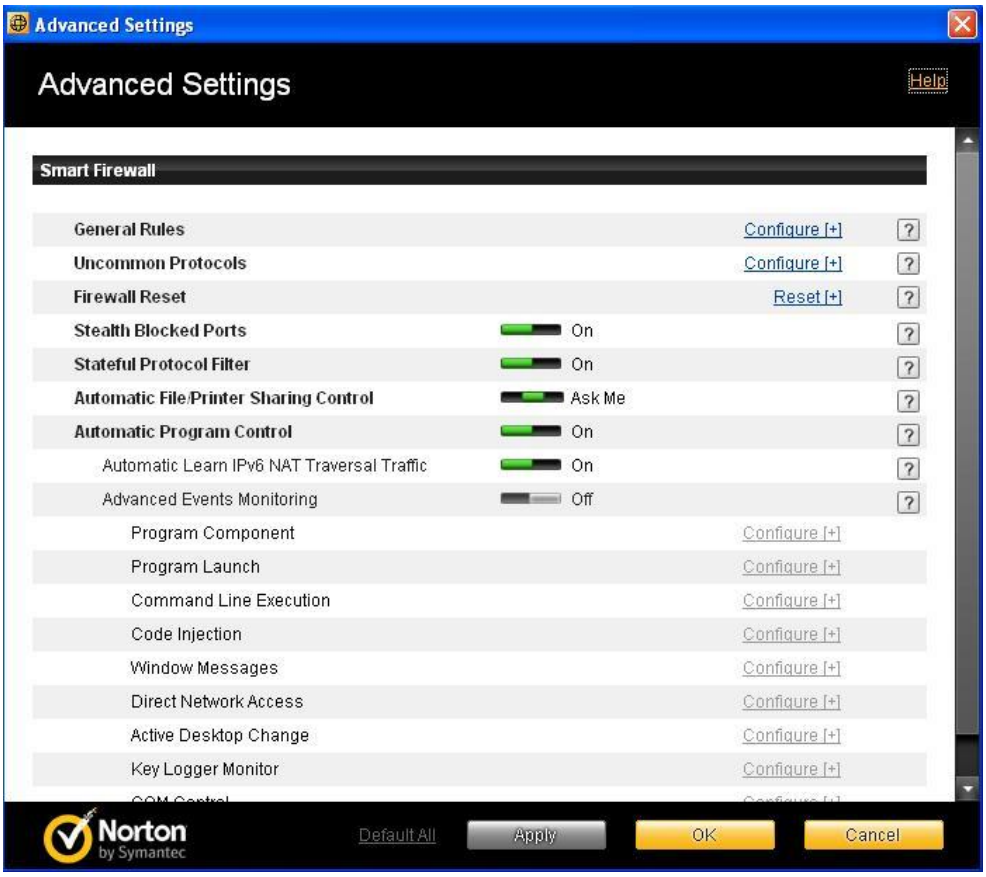
در این پنجره با انتخاب گزینه ی Block و تیک زدن گزینه ی Protocol می توانیم پورتی که می خواهیم آن را مسدود نماییم را وارد کنیم . و بر روی Ok کلیک نماییم .

بستن پورت در Norton internet Security

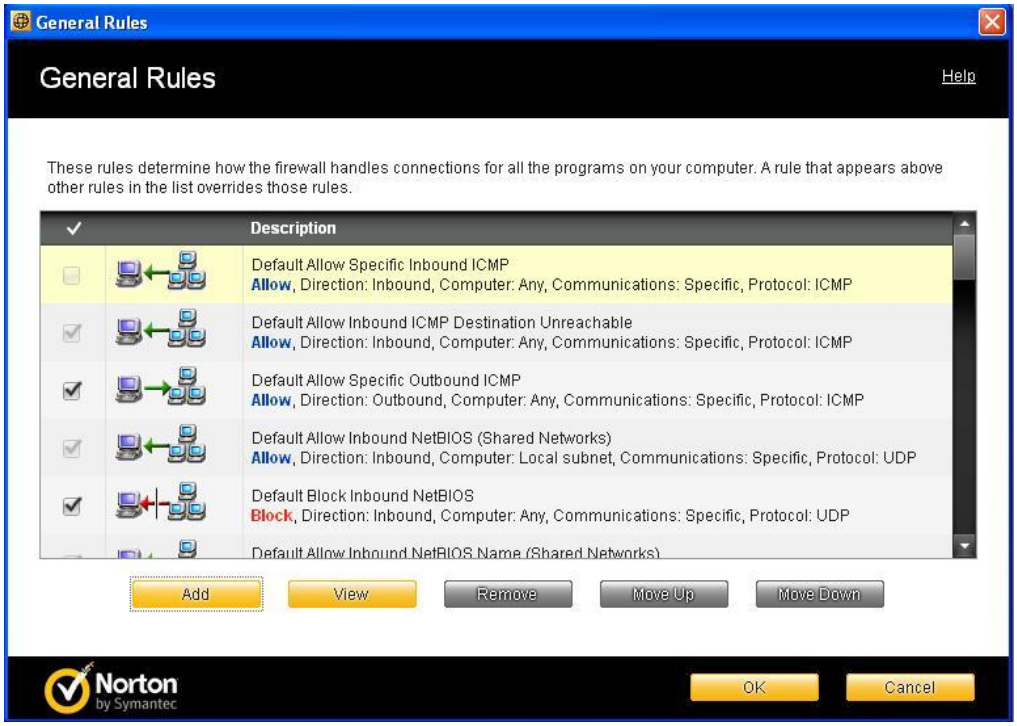
یکی دیگر از فایروال های قوی در ضمینه ی حفاظت از سیستم های کامپیوتری Norton Internet Sec می باشد . جهت بستن پورت در این نرم افزار وارد برنامه شوید .



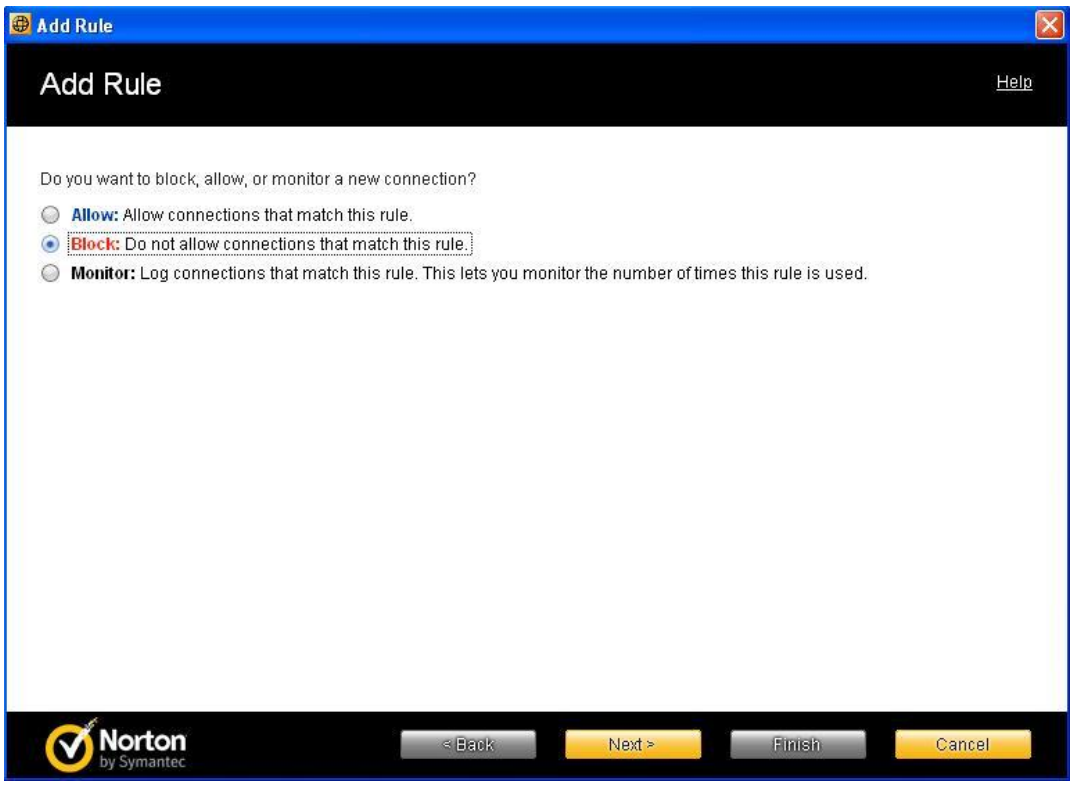
در این پنجره در قسمت Network Setting بر روی Advanced Setting کلیک نمایید .



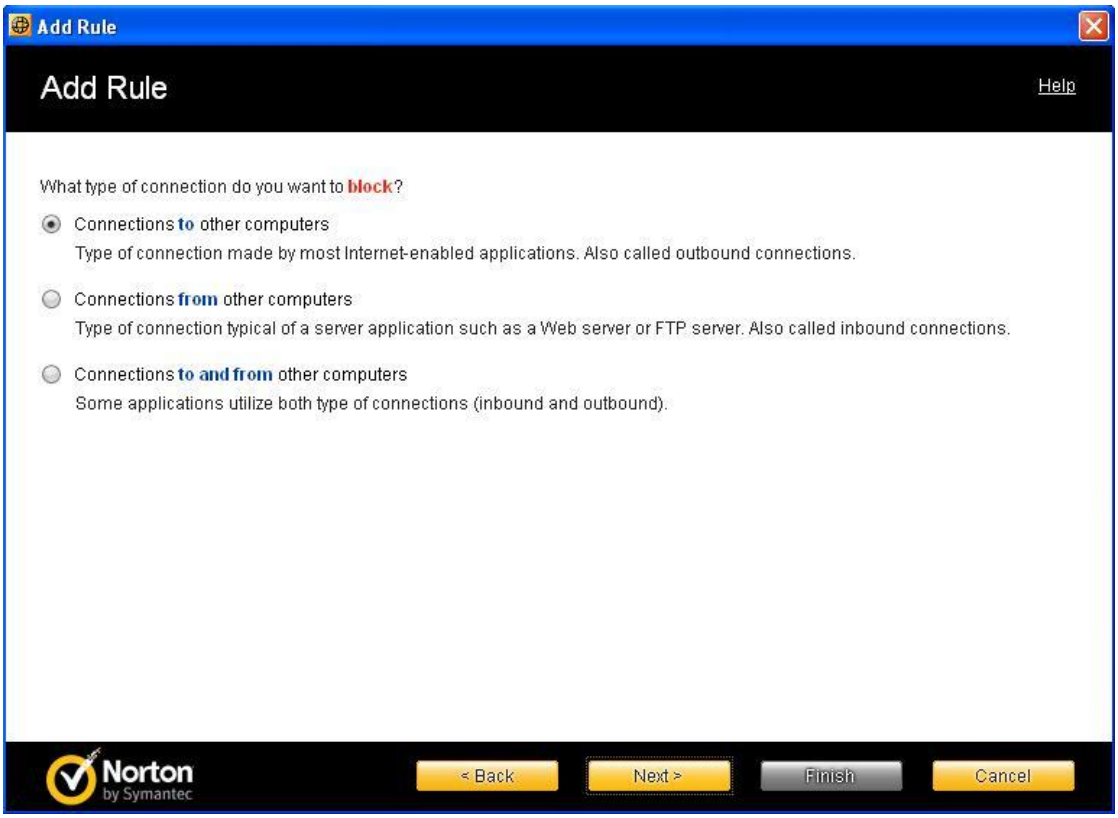
در پنجره ظاهر بالا گزینه ی Generall Rulles را انتخاب نمایید .



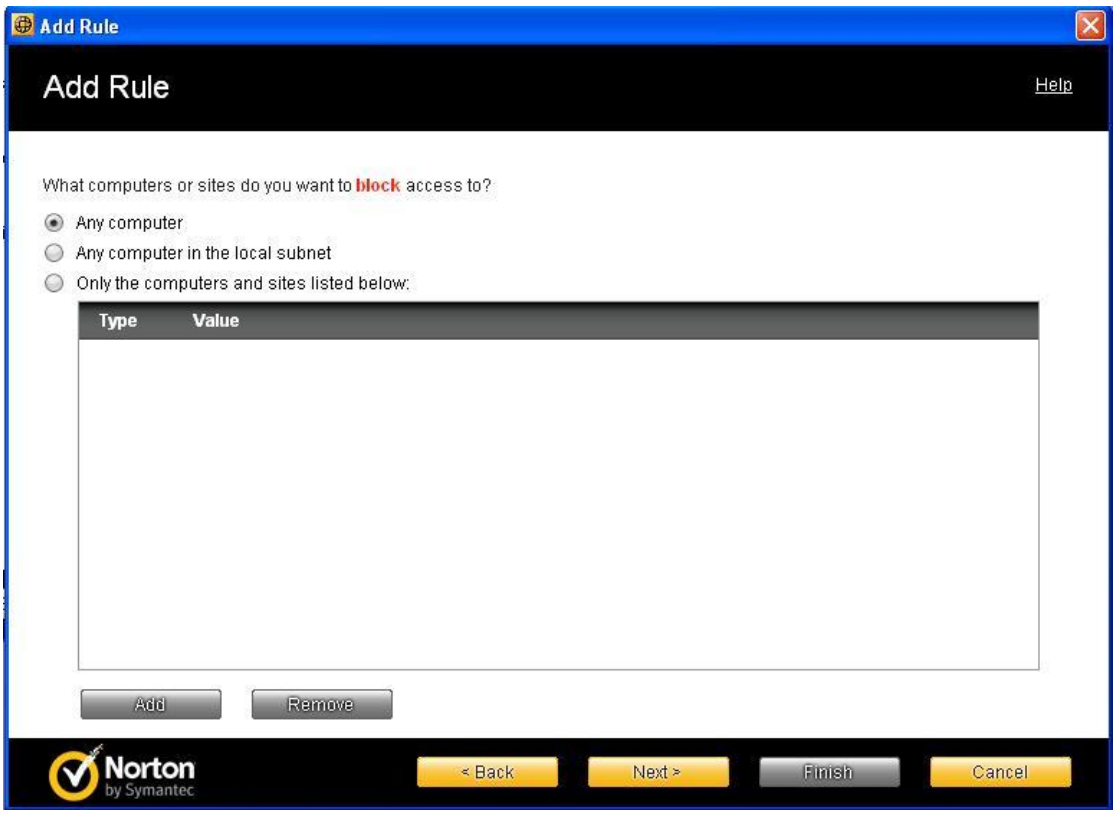
در این پنجره بر روی Add کلیک نمایید



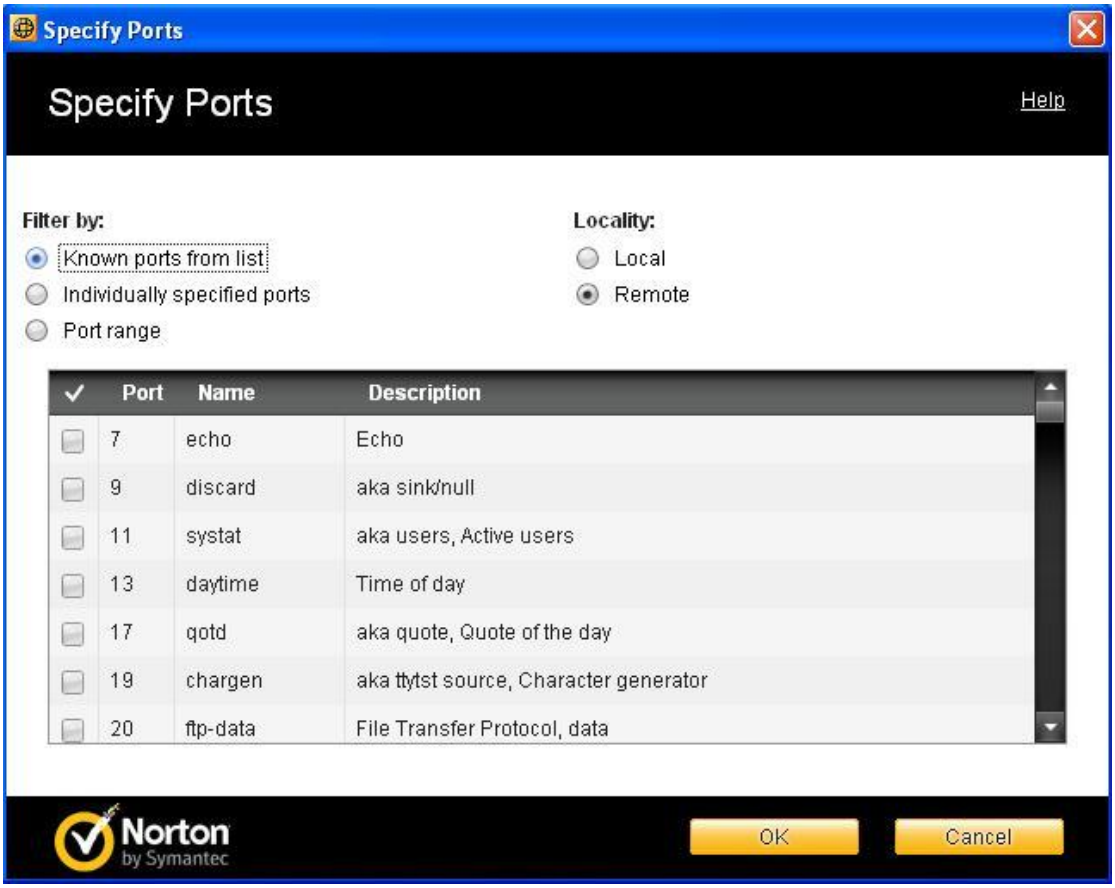
در این قسمت جهت مسدود کردن پورت بر روی Block کلیک نمایید و به مرحله ی بعد بروید



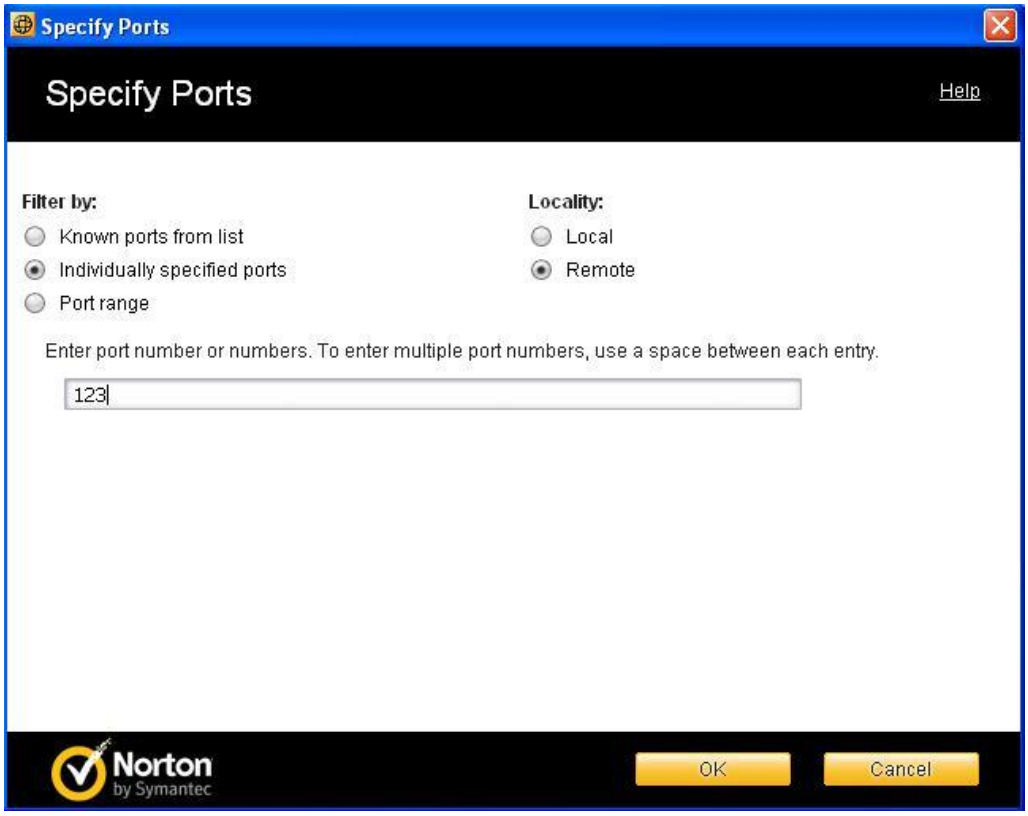
در این قسمت یکی از گزینه ها را انتخاب کنید (بر طبق نیاز) و به مرحله ی بعدی بروید .



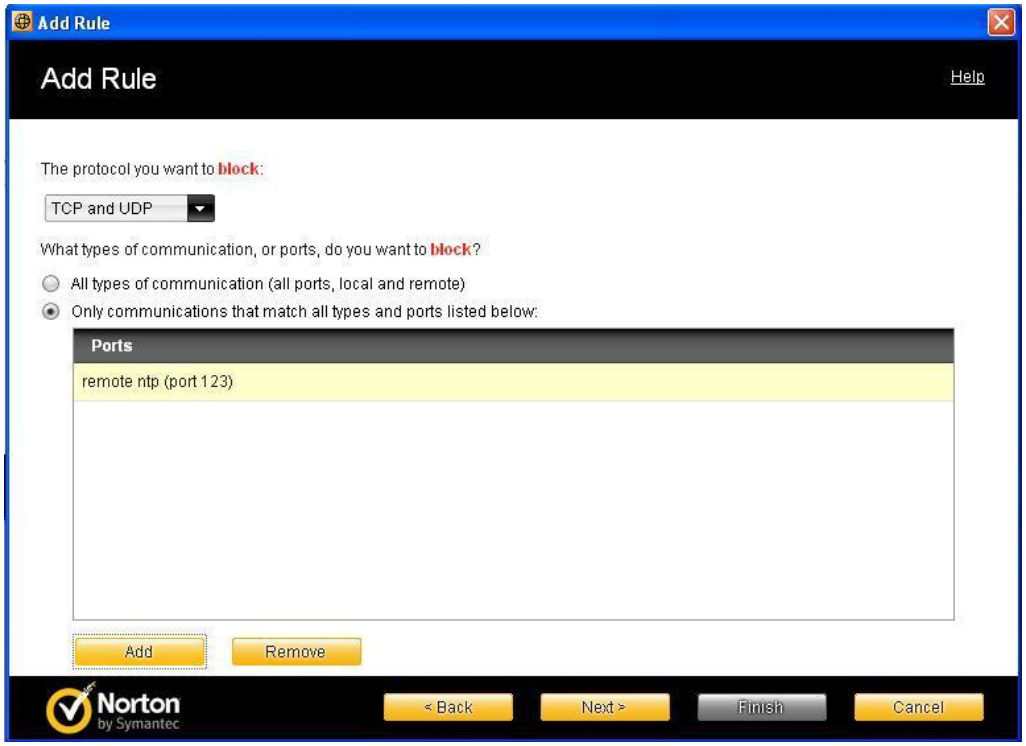
در این مرحله هم Next را زده



تا به این قسمت برسیم در اینجا می توانیم با انتخاب گزینه ی اول لیستی از پورت های معذوف که مربوط به سرویس هه می باشند را مشاهده نمایمم و بر روی آن کلیک کنیم تا بسته شوند و اگر پورت مورد نظر بین گزینه های زیر نبود میی توانیم با انتخاب گزینه ی دوم آن را جهت مسود سازی وارد نماییم



و نوع آن را مشخص می کنیم و با انتخاب Ok پورت ۱۲۳ بر روی سیستم شما مسدود می شود .



بستن پورت از طریق کد های VBS

VBS یا همان ویژوال بیسیک اسکریپت یک زبان برنامه نویسی ساده برای ویندوز می باشد که بااستفاده از برنامه Wscript قابل اجرا می باشد این کد های به کار رفته در این زبان همان کد های ویژوال بیسیک می باشد به همین دلیل این اسم را روی آن گزاشته اند . در ویندوز این زبان قدرت فراوانی را در تغییر اجزای مختلف آن دارد حتی ویروس های زیادی هم با این زبان نوشته شده است . اینجا اسکریپ هایی را با استفاده از این زبان معرفی می کنیم که بتوانید با اجرای آن روی پورت ها مدیریت کنید .

جهت باز کردن یک پورت

```
Set objFirewall = CreateObject("HNetCfg.FwMgr")
Set objPolicy = objFirewall.LocalPolicy.CurrentProfile
Set colPorts = objPolicy.GloballyOpenPorts

Set objPort = colPorts.Item(9999,6)
objPort.Enabled = TRUE
```

جهت بستن یک پورت

```
Set objFirewall = CreateObject("HNetCfg.FwMgr")
Set objPolicy = objFirewall.LocalPolicy.CurrentProfile

Set colPorts = objPolicy.GloballyOpenPorts
errReturn = colPorts.Remove(9999,6)
```

Author : moslem haghighian

Kurd Black Hat Security Team

Email :

l4tr0d3ctism@yahoo.com

l4tr0d3ctism@gmail.com

l4tr0d3ctism@hotmail.com

Iranian Black Hat group

Greyh4t.com/cc

Black-hg.com/cc