# انواع حملات توسط هکر ها

۱ -حمله به روش (Denial of Service Attack) DoS ۲ -حمله به روش Exploit ۳ -حمله به روش) Info Gathering تلنت کردن يكي از مثالهاي آن است ) ۴- حمله به روش Disinformation Telnet و آشنايي بيشتر با اين دستور Telnet :در اصل پروتكلي است كه براي loginو استفاده از يک كامپيوتر ديگر به كار مي رود .روش اجراي Telnet در لينوكس يا انواع ديگر Unix و نيز ويندوز 2000 تا حد خيلي زيادي شبيه چيزي است كه ما گفتيم. براي آشنايي بيشتر با telnet و گرفتن جواب دقيقتر سوالات بالا روي مـــن كليک كنيد كه به يک ميزبان واقعي Telnet شما را متصل مي كند كه مي توانيد به رايگان عضو شويد و از خدمات آن استفاده كنيد. خواهيد ديد كه لينک فوق در حقيقت Hyper Terminal را باز مي كند. در حقيقت هم اگر به درون Hyper Terminal برويد مي توانيد در قسمت برقراري تماس با انتخاب TCP/IP مستقيما از آن به عنوان Telnet استفاده كنيد. اما اينكه Telnet در هک چه نقشي داره و چه فايده اي داره كلاً رو از زبان "كارولين مينل" برايتان مي نويسم: "فقط با يک سرويسگير] Telnet مثل همين Telnet خودمون در ويندوز] شما مي توانيد: · ايميل بفرستيد. · سورس (متن برنامه) سايتها را بخوانيد. · به ميزبانهاي وب ورودیهاي غير منتظره بفرستيد كه مي تواند سبب دريافت پاسخهاي شگفت انگيز و گاهي غير قانوني شود. · به بسياري از ديگر سرويسهاي كامپيوترهاي ميزبان وب ورودي دلخواه خود را بدهيد. · در سرويسهايي كه ميزبانها، روترها و حتي كامپيوترهاي شخصي مردم در منزلشان در اختيار شما مي گذارند كاوش و جستجو كنيد." تلنت كردن معمولا اولين كاري است كه يک هكر براي هک كردن يک سايت انجام ميدهد، زيرا بعضي از پورتها در صورت بسته نبودن روي آن سرور، معمولا حاوي اطلاعات بسيار مهمي هستند.(به همين دليل ما بايد اول پورتها رو چک كنيم بعد telnet چون اگر پورتي كه ما بهش telnet ميكنيم close باشه دستور اجرا نميشه) موضوع مهمي كه يك نفوذ گر واقعي به آن توجه مي كند در سه اصل خلاصه شده است : ۱- او هيچگاه سعي در استفاده از برنامه هايي كه ديگران نوشته اند نمي كند ... »البته ممكن است تعدادي از هكر ها باشند كه با استفاده از تروجان ها يا Back doors ها به اين كار بپردازند و فقط خود را با اين مباحث ساده درگير كنند. 2- معمولا از به كارگيري برنامه هاي گرافيكي كه حتي خود طراحي كرده اند نفرت دارند و فقط در دنياي سياه و سفيد msdos-prompt براي خود حكومت تشكيل ميدهند.(در اصل از استفاده نرم افزار براي هک نفرت دارند) 3- موضوع سوم و اساسي اين است كه فقط يك چيز را در دنيا ميشناسند و آن هم تايپ كردن است.تايپ در صفحه سياه و سفيد . command prompt در ويندوزXP ، يكي از بهترين ابزارهايي كه در دست شماست، همان صفحه مشكي Command prompt است. در ويندوز XP دو نوع DOS وجود دارد. يكي cmd.exe و ديگري command.comكه cmd.exe براي كارهاي ما مناسبتر است و كليک روي دگمه Start و انتخاب All programs و انتخاب Accessories و سپس كليک روي Command prompt نيز همين را باز خواهد كرد. (راه مناسبتر: دگمه ويندوز كيبورد را به همراه حرف R فشار دهيد، تايپ كنيد cmd و Enter كيبورد را فشار دهيد). تايپ كردن Help و فشردن Enter ليستي از دستورات را براي شما به نمايش در مي آورد كه متاسفانه دستورهاي مناسب براي هک را از قلم انداخته است) .ناگفته نماند كه Help ويندوز XPاگر بدانيد كه در كجاي آن به دنبال چه بگرديد نسبتاً كامل است). از جمله مهمترين اين دستورها مي توان به دستورات زير اشاره كرد : TCP/IP command: telnet, netstat, nslookup, tracert, ping, ftp NetBIOS commands: nbtstat, net use, net view, net localgroup ( و چند دستور ديگر) در اين شماره، براي اينكه هم كمي با) telnet كه به عنوان يكي از مهمترين ابزارهاي هک مطرح بوده و هست (آشنا شويد هم از موضوعي شروع كرده باشيم كه ملموس و جذاب باشد، فرستادن ايميل از طرف هركسي به هركسي با telnet را آموزش مي دهيم (من هم مي دونم كه راههاي آسونتري براي اين كار هست و راحتترين راهش استفاده از Outlook مايكروسافت است، اما مطمئنم از ديدن پشت صحنه نمايش فرستادن ايميل لذت خواهيد برد). قبل از هر چيز بگم كه telnet كردن به خودي خود جرم نيست و استفاده از telnet براي فرستادن يا گرفتن ايميل نه ضرري براي شما دارد و نه ميزبان. اما شما اين حق را نداريد كه از طرف كسي به كس ديگر ايميل بزنيد مگر با اجازه آنها.اول وارد صفحه سياه خط فرمان شويد (مراحل نوشته شده در بالا)، حالا مي خواهيم از دستور telnet استفاده كنيم telnet : target portبه جاي target آدرس سايت يا كامپيوتر و به جاي port بايد آدرس پورت را وارد كنيد. در مثال اين شماره با فرستادن ايميل (smtp)سروكار داريم كه پورت آن 25 است و آدرس نيز آدرس يک سرور ايميل بايد باشد. به عنوان مثال telnet mail.hamsafar.com 25 را خواهيم داشت. همسفر، وب سايت من كه عضويت در آن را به شما توصيه مي كنم، فقط يک مثال است و شما مي توانيد از هر آدرس مشابهي استفاده كنيد. جوابي دريافت خواهيد كرد كه معمولا شامل نام ميزبان ايميل است. حالا وقت سلام كردن با دستور helo است (دستور ehlo هم داريم كه مي توانيد امتحانش كنيد). بهتر است جلوي helo آدرس ايميل فرستنده را درج نماييد. با گرفتن جواب سلام، براي فرستادن ايميل از دستور mail استفاده مي كنيم [email]leyli@masalan-ye-sity.com[/email] mail from:بعد از گرفتن OK حالا گيرنده را معرفي مي كنيم [email]majnoon@hamsafar.com[/email] rcpt to: :اين بار بعد از گرفتن OK دستور data را تايپ و Enterكنيد. توجه كنيد كه ميزبان به شما مي گويد وقتي كارتان تمام شد . بزنيد كه اين يعني زدن يكEnter ، تايپ كردن يک نقطه و دوباره زدن .Enter حالا وقت وارد كردنSubject ، toو from و سپس زدن دو Enter و وارد كردن متن ايميل و سپس زدنEnter ، تايپ كردن نقطه و زدن Enter دوم است. در عكس بالا فقط Subject وارد شده است. نمونه كاملتري كه شامل To و From مي باشد به صورت زير است: data 354 ok, send it; end with . From: [email]Leyli@masalan-ye-sity.com[/email] To: [email]Majnoon@hamsafar.com[/email] Subject: Salam! In email faghat be ghasde azmayesh ferestade shode ast. Rooze khooby dashte bashid . 250 Message queuedبه تفاوت اين دو مورد در عكس زير توجه كنيد: توجه كنيد كه همسفر فقط به شما اجازه خواهد داد به آدرسهايي كه به hamsafar.com ختم مي شوند ايميل بزنيد. اگر تمايل به خريد ايميل روي همسفر & webmail) (pop3را داريد، با ما به آدرس [email]sales@hamsafar.com[/email] مكاتبه كنيد. اما دستوراتي كه گفته شد روي هر ميزباني كار خواهد كرد. به احتمال زياد جايي كه از آن اينترنت گرفته ايد اگر درخواست ايميل POP3 از آنها بكنيد به رايگان به شما خواهند داد و شما آدرسي كه به عنوان SMTP يا Outgoing server از آنها دريافت مي كنيد را به جاي mail.hamsafar.com خواهيد نوشت. در هر صورت شما اين اجازه را داريد كه با روش فوق با من به آدرس [email]ehssanr@hamsafar.com[/email] مكاتبه كنيد و به اين شكل روش را آزمايش كنيد. به ياري خدا در شماره آينده با آموزش نحوه نصب و استفاده از ميزبان SMTP خود ويندوزXP ، خواهيد آموخت كه چگونه بي نياز از هر SMTP ايميل بفرستيد. حالا كه به اينجا رسيديم اميدوارم اين سه سوال براي شما پيش آمده باشد كه اگر جوابشان را هم مي دانستيد كه هيچ وگرنه ما به آنها جواب مختصر و مفيد خواهيم داد. اگر هم هيچ سوالي برايتان پيش نيامده اين قسمت را باز هم به دقت بخوانيد چرا كه مهمترين مفاهيم را به سادگي توضيح داده ايم. باز هم تاكيد مي كنم كه اين سه سوال و پاسخ آنها را با دقت بخوانيد و بفهميد. چند نكته مهم : سوال : اسم Target كه در قالب Telnet target port مطرح كرديم چيست و چرا برخي به جاي آن 4 تا عدد مي زنند؟ پاسخ: هر كامپيوتر روي اينترنت با 4 عدد بين 0 تا 255 كه با نقطه از هم جدا مي شوند مشخص مي شود. در XP براي فهميدن IP خود كافي است كه روي مانيتورهاي نشاندهنده اتصال شما به اينترنت دابل كليک كنيد و از بالاي پنجره ظاهر شده با انتخاب قسمت جزئيات (Details) آدرس IP خود را خواهيد ديد.(براي كساني كه ويندوز قديمي دارند معمولا يک راه مناسب تايپ كردن winipcfg در پنجره Run و فشردن Enter است). حال وقتي كه كسي يک Domain ثبت مي كند، در واقع روي اين عددها يک اسم مي گذارد. اين كار دو فايده اساسي دارد. يكي اينكه اگر عدد فرد به هر دليل عوض شود لازم نيست دوباره به همه خبر دهد و دليل ديگر آن اين است

که اسم ساده تر به خاطر سپرده مي شود و احتمال اشتباه در آن کمتر است. همانطور که مي بينيد تشبيه IP به شماره تلفن تا حدي به فهم آن کمک خواهد کرد. در اينجا قصد نداريم وارد بحث دقيق IP بشويم اما دو عدد اول IP حتما به اينکه از کجا اينترنت داريد مربوط است و به طور تئوري با داشتن IP شما مي توان مکان شما را به صورت فيزيکي هم در روي کره زمين مشخص کرد. براي دانستن IP يک سايت کافي است که از داخلCommand Prompt ، دستور Ping را اجرا کنيد. به سادگي تايپ کنيد Ping yahoo.com يا Ping hamsafar.comتا IP را ببينيد. پس حالا ديديد که در واقع منظور از Target شماره آن کامپيوتري است که قصد داريد به آن متصل شويد. (مفهوم Port و کمي از پروتکل (Telnet: سوال : اصطلاح port که در قالب Telnet target port مطرح کرديم چيست و چرا ما آنرا برابر 25 گرفتيم؟ اگر جاي آن را خالي بگذاريم چه مي شود؟ ترجمه کلمه port به فارسي "بندر" مي شود .کامپيوتر مقصد را به صورت جزيره اي تصور کنيد که چندين بندر دارد و هرکدام تخصص خاص خود را دارند. يکي براي نفتکشهاست يکي براي صادرات سنگ معدن و Port . ... روي کامپيوتر هم در حقيقت همچين مفهومي داره Port .کامپيوتر جايي است که اطلاعات مي توانند از آن خارج يا به آن وارد شوند. کيبورد، پرينتر، نمايشگر و مودم از پورتهايي هستند که به راحتي از آنها درک فيزيکي داريد اما پورتهاي مجازي توسط نرم افزار ايجاد مي شوند. وقتي پورت مودم شما به اينترنت متصل مي شود، کامپيوتر شما مي تواند هر کدام از پورتها را که تعدادشان بيش از 65000 عدد است ببندد يا باز بگذارد و نيز مي تواند به هر کدام از اين پورتهاي يک کامپيوتر ديگر متصل شود (البته در صورتي که آن کامپيوتر بر روي اين پورت چيزي در حال اجرا داشته باشد و نيز ديوارآتش (firewall) آن را نبسته باشد. (در ويندوز XP هنگامي که اينترنت خود را تنظيم مي کنيد اين امکان را به شما مي دهد که با استفاده از ديوار آتش جلوي نفوذ ديگران به شما را بگيرد که به طور پيش فرض خودش آنرا فعال مي کند). پورتهاي خاص کاربردهاي خاص دارند. پورت 25 معمولا براي) SMTP مخفف ( Simple mail transfer protocol است و ما براي ارسال ايميل از آن استفاده کرديم. اگر قصد دريافت ايميلهايمان را داشتيم به چورت 110 سر مي زديم، براي مشاهده صفحات وب به سراغ پورت 80 مي رويم و... (درست حدس زديد Outlook !هم به طور پيش فرض براي ارسال ايميل از پورت 25 و براي دريافت آن از پورت 110 استفاده مي کند و اينترنت اکسپلورر هم به پورت 80 شماره IP آدرس سايتي که مي نويسيد سر مي زند.) و در پايان اگر پورت را ننويسيد، پورت برابر 23 فرض مي شود که پورت Telnet است. به پاسخ سوال اول دوباره سر بزنيد. وقتي روي لينکي که داده ام کليک مي کنيد در حقيقت به پورت 23 آن ميزبان متصل مي شويد. امروزه بسياري از سايتها بخصوص سايتهايي که از ميزباني ويندوزي استفاده مي کنند سرويس Telnet ندارند و امکان اتصال به پورت 23 وجود ندارد اما من باز هم توصيه مي کنم که براي تجربه Shell Accountهم که شده Telnet واقعي را تجربه کنيد. اين Telnet در حقيقت معمولا يک BBS هم هست اما امکانات بسيار زيادي هم براي يک هکر دارد. براي آشنايي اوليه صرف اينکه کمي انگليسي بفهميد و هرموقع گير کرديد تايپ کنيد Help و Enter کنيد بايد کافي باشد. سوال :آدرس مورد استفاده در Telnet براي سايتهاي مختلف را چگونه پيدا کنيم؟ پاسخ:اگرچه بسياري از سايتها از همان-mail.domain name.comاستفاده مي کنند، اين امر همه گير نيست. در ويندوز و با استفاده از cmd.exe خودمان به راحتي مي توانيم اين آدرس را براي 99% دومينها تعيين کنيم. پس از اجراي cmd ، دستور nslookup را با تايپ کردن اين کلمه و فشردن Enter اجرا کنيد. از آنجايي که ما قصد گرفتن اطلاعات در مورد سامانه دريافت ايميل آن سايت را داريم، از کد mx که مخفف mail exchanger است استفاده مي کنيم. به طور کلي اطلاعات يک domain شامل چند قسمت است که براي مورد ما فقط اين اطلاعات مورد نياز است. پس تايپ کنيد set q=mx و Enter را فشار دهيد. حال کافي است نام domain را تايپ و Enter کنيد. در برخي موارد مانند مثال زير فقط يک جواب مي گيريد < : irib.com Server: UnKnown Address: 213.165.123.1 irib.com MX preference = 60, mail exchanger = mail.irib.com mail.irib.com internet address = 62.220.119.60و يا مثال زير irna.com MX preference = 10, mail exchanger = irna.com : irna.com nameserver = ns1.gpg.com irna.com nameserver = ns1.irna.net irna.com nameserver = ns1.simorgh.com irna.com nameserver = ns2.irna.net irna.com internet address = 209.1.163.101 ns1.irna.net internet address = 217.25.48.18 ns1.irna.net internet address = 194.126.61.8 ns2.irna.net internet address = 194.126.61.7 ns2.irna.net internet address = 217.25.48.17که نشان مي دهد براي آدرس irib.com بايد از mail.irdir.com استفاده کرد و براي آدرس irna.com بايد از irna.com استفاده کرد. به قسمت قرمز رنگ دقت کنيد. هميشه پاسخ مورد نظر ما بعد از عبارت mail exchanger قرار مي گيرد. گاهي تعداد جوابها بيشتر است hamsafar.com MX preference = 10, mail exchanger = mail.hamsafar.com hamsafar.com MX : preference = 15, mail exchanger = hamsafar.com mail.hamsafar.com internet address = 38.118.143.98 hamsafar.com internet address = 38.118.143.98و يا مثال زير hotmail.com MX preference = 5, mail exchanger = mx4.hotmail.com : hotmail.com MX preference = 5, mail exchanger = mx1.hotmail.com hotmail.com MX preference = 5, mail exchanger = mx2.hotmail.com hotmail.com MX preference = 5, mail exchanger = mx3.hotmail.com hotmail.com nameserver = ns1.hotmail.com hotmail.com nameserver = ns2.hotmail.com hotmail.com nameserver = ns3.hotmail.com hotmail.com nameserver = ns4.hotmail.com mx4.hotmail.com internet address = 65.54.254.151 mx4.hotmail.com internet address = 65.54.253.230 mx1.hotmail.com internet address = 65.54.254.129 mx1.hotmail.com internet address = 65.54.252.99 mx1.hotmail.com internet address = 65.54.166.99 mx2.hotmail.com internet address = 65.54.254.145 mx2.hotmail.com internet address = 65.54.252.230 mx2.hotmail.com internet address = 65.54.166.230 mx3.hotmail.com internet address = 65.54.254.140 mx3.hotmail.com internet address = 65.54.253.99 ns1.hotmail.com internet address = 216.200.206.140 ns2.hotmail.com internet address = 216.200.206.139 ns3.hotmail.com internet address = 209.185.130.68 ns4.hotmail.com internet address = 64.4.29.24و يا مثال زير cnn.com MX preference = 10, mail exchanger = atlmail4.turner.com cnn.com MX : preference = 20, mail exchanger = atlmail2.turner.com cnn.com MX preference = 30, mail exchanger = nymail1.turner.com cnn.com MX preference = 10, mail exchanger = atlmail1.turner.com cnn.com nameserver = twdns-04.ns.aol.com cnn.com nameserver = twdns-01.ns.aol.com cnn.com nameserver = twdns-02.ns.aol.com cnn.com nameserver = twdns-03.ns.aol.com atlmail1.turner.com internet address = 64.236.240.146 atlmail4.turner.com internet address = 64.236.221.5 atlmail2.turner.com internet address = 64.236.240.147 nymail1.turner.com internet address = 64.236.180.95اگر کمي دقت کنيد، قسمت MX preference همواره داراي يک عدد است. اگر جوابهاي متفاوتي پيدا شد، جوابي که عدد MX preference آن کمتر باشد به طور معمول انتخاب مناسبتري است و بايد اولين جوابي باشد که امتحان مي کنيد. با اين روش شما مي توانيد بدون استفاده از SMTPخاصي ايميلهاي خود را ارسال کنيد يا برنامه اي بنويسيد که ايميل ارسال کند. سوالي که در اينجا پيش مي آيد اين است که چه کارهايي در اين زمينه مجاز و چه کارهايي غيرقانوني است. فرستادن ايميل به هزاران نفر طوري که به هر کدام فقط يک ايميل برسد و آنها راهي براي خروج از ليست شما داشته باشند غيرقانوني نيست اما ممکن است ISP يا Host شما را عصباني کند، بنابراين بهتر است از آنها سوال کنيد يا حداقل مطمئن باشيد که در قراردادي که با آنها امضا کرده ايد ممنوعيت اين مورد ذکر نشده باشد. البته اگر اين ايميل طوري فرستاده شود که فرستنده آن صحيح نباشد و به نظر برسد که از طرف کس ديگري آمده است قابل پيگرد قانوني است و افراد زيادي در دنيا به اين دليل محاکمه شده اند. فرستادن چندين ايميل به يک فرد طوري که سبب مزاحمت وي يا از دست رفتن برخي از اطلاعات وي شود جرو است و از طريق مراجع ذيصلاح قابل پيگرد قانوني مي باشد. فرستادن ايميل طوري که به نظر برسد از

آدرسي ديگر آمده است، اگر آن آدرس ديگر متعلق به شما نباشد علاوه بر غير اخلاقي بودن عمل، انشاءالله قابل پيگيري قانوني مي باشد. از توضيح نصب و كار با SMTP روي ويندوز شخصي منصرف شديم، اما همين قدر بدانيد كه از control panel-> add/remove programsبايأ به قسمت add/remove windows components برويد و از آنجا IIS و Message queuing را نصب كنيد و سپس در صورت نياز آنها را تنظيم كنيد. به اين شكل شما قادر به فرستادن ايميل با telnet كردن به آدرس localhost يا آدرس IP 127.0.0.1 به هر آدرسي خواهيد بود. اميدوارم بعد از خواندن اين صفحات به اين نتيجه رسيده باشيد كه هركسي به راحتي مي تواند هر ايميلي را از طرف كس ديگري براي شما ارسال كند و در مورد ايميلهاي مشكوک بايد احتياط كنيد. البته مشكلات ايميل به اينجا ختم نمي شود... ايميل را به طور معمول به كارت پستال بدون پاكت تشبيه مي كنند به اين مفهوم كه در مسير رايانه شما به رايانه گيرنده نامه در تمام مسيرهاي مياني و توسط پستچيها قابل خواندن است! اگرچه متاسفانه در ايران به دليل اهميت ندادن به امنيت اطلاعات، تمامي مكالمات تلفني (بخصوص تلفن همراه)، فكس و مانند آنها هم همين حكم را دارند و در مقايسه وضع ايميل كمي بهتر است (بعد بگيد چرا تجارت الكترونيكي نداريم... يا بگيد چرا بانكها خودشون برا خودشون شبكه راه مي اندازند يا...)! سوال: جگونه مي شود به يک پورت باز telnet كرد؟ پاسخ:براي اينكه عملكرد يک پورت براي شما روشن شود، بايد به آن پورت Telnet كنيد.البته معمولا تعدادي از پورتهايي را كه ممكن است اطلاعاتي مهم را در اختيار هكرها قرار دهند مثل پورت ۷۹ يا ۸۰ معمولا بسته است و ارتباط با آنها شايد برقرار نشود. براي telnet كردن در command prompt دستور زير را تايپ كنيد telnet hostname portnum :در اين دستور بهجاي hostname شماره ip و يا نام سايت را وارد ميكنيد و بهجاي portnum شماره پورت توجه كنيد كه فقط در صورتي ميتوانيد با يک پورت تلنت كنيد كه ان پورت open باشد . مثلا براي تلنت كردن به پورت ۱۳ كه ساعت و تاريخ را بهدست ميدهد در كامپيوتري با IP ۱۹۲.۱۶۸.۱۰۰.۳۵ : telnet مينويسيد 192.168.100.35 13يا اگر ip سايت مورد نظر رو بلد نبوديد (بعد روش بدست اوردن ip رو هم ميگم) ميتوانيد از اين راه استفاده كنيد : telnet yahoo.com 13دستور Netstat و استفاده از اين دستور اين دستور كه با سويچ هاي ديگري هم استفاده ميشه يكي از دستورايي هست كه همه هكر ها اول باهاش آشنا ميشن.كه با تايپ اين دستور شما متوجه آي پي سيستمها و پورتهايي كه با آنها در ارتباط هستيد ميشويد و مشاهده ميكنيد كه چه پورتهايي Listening و يا Established هستن اين باعث ميشود اگر پورتي مخصوص يک تروجن مثل 27374 كه پورت اصلي Sub7 هست در سيستم شما باز بود شما متوجه اين پورت باز بروي سيستمتان بشويد. اگر در قسمت Foreign Address هم يک آي پي بوسيله پورتي به سيستم شما وصل بود شما به سرعت متوجه مي شويد كه يک نفر با آن آيپي در سيستم شماست ، پس اين راهيست كه متوجه گرديد سيستمتان آسيب پذير است يا نه ، براي مثال من با تايپ دستور Netstatدر Ms-Dos پس از اتصال به اينتر نت نتايج زير را گرفتم C:WINDOWS>netstat Active Connections Proto Local Address : Foreign Address State TCP Midia:1454 cs33.msg.sc5.yahoo.com:5050 ESTABLISHED TCP Midia:1488 63.123.44.222:80 ESTABLISHED TCP Midia:1491 opi1.vip.sc5.yahoo.com:80 TIME_WAIT TCP Midia:1497 64.187.54.23:80 ESTABLISHED TCP Midia:1498 64.187.54.23:80 ESTABLISHEDهمانطور كه ملاحظه ميكنيد اين دستور گاهي اوقات اسم صاحب سيستم كلاينتي كه شما با آن در ارتباط هستيد را نيز ميدهد و چون اينجا من با كسي در PM نبودم اسم كسي را نميبينيد ولي اگر كسي با من چت كند و دستور Netstat را اجرا كند اسم را ميبيند و متوجه ميشود كه Midiaصاحب آن سيستم كلاينتي مي باشدكه در حال چت كردن با آن است و همچنين در اين قسمت مشخص است كه من با پورت 5050 با ياهو مسنجر ارتباط برقرار كرده ام و نيز نتايجي كه در زير Local Addressمشخص است اطلاعاتي درباره خود من مي باشد . و نتايجي كه در Foreign Address بدست مياد مشخص ميكند كه ما با چه سرور يا كلاينتي در ارتباط هستيم . كه در سطر پنجم مثال بالا يعني 63.123.44.222:80 آيپي سايت ياهو ميباشد و مشخص ميكند كه من در سايت ياهو بوده و به وسيله پورت 80 كه پورت Http ميباشد با اين وب سرور ارتباط برقرار كرده ام و در قسمت Status هم مشخص ميشود كه شما با چه پورتهايي Established هستيد يعني ارتباط برقرار كرده و وصل هستيد و چه پورتهايي Listening يا منتظر Requestو در حال شنيدن مي باشيد ، بنابراين با دستور Netstat مي شود يک عمل مانيتورينگ از تمام آيپي ها - پورتها و ماشينهايي كه شما با آنها در ارتباط هستيد گرفت . دستور Netstat/? : Help برنامه Netstat را معرفي ميكند و سويچ هاي كه ازش ميتوان استفاده كرد و در مقابل هر سويچ در مورد كار آن توضيح مختصري ميدهد. دستور : Netstat -n با اين دستور ميتوان آيپي و پورت سيستمي كه شما با آن در ارتباط هستيد را بدست آورد . براي مثال وقتي شما با يک نفر در ياهو مسنجر چت ميكنيد پورت ۵۰۵۰ روي سيستم open هست چون ياهو از پورت ۵۰۵۰ استفاده ميكند پس با تايپ netstat -n خواهيد داشت Active Connections Proto Local Address : Foreign Address State TCP 217.219.223.21:1425 216.136.175.226:5050 TIME_WAIT TCP 217.219.223.21:1431 64.242.248.15:80 ESTABLISHED TCP 217.219.223.21:1437 217.219.223.38:5101 ESTABLISHEDهمانطور كه ملاحظه ميكنيد من در اين لحظه با آيپي 217.219.223.38 در حال چت كردن بودم كه اشتراكش هم از رايان روش بوده (مثل خودم)و آي پي خود نيز پروتكلي كه ما بوسيله آن با يک سيستم ارتباط برقرار كرديم Proto مشخص ميشود در قسمت Local Address من همTCP ارتباط برقرار شده است. دستور : Netstat -na با تايپ كردن اين دستور در MS-DOS Prompt تمام پورتهايي كه داده ها و بسته ها را ميفرستند مشخص ميشود ، نشان " na " در تمام دستورات به معني نمايش همه پورتها و ليست كردن آدرسهاي شبكه و شماره فرمها در يک قالب عددي مي باشد ، براي مثال من با تايپ اين فرمان در MS-DOS اين نتايج را گرفتم C:WINDOWS>netstat -na Active : Connections Proto Local Address Foreign Address State TCP 0.0.0.0:1954 0.0.0.0:0 LISTENING TCP 0.0.0.0:5101 0.0.0.0:0 LISTENING TCP 217.219.223.21:1954 207.46.106.21:1863 ESTABLISHED TCP 217.219.223.21:1971 216.136.225.36:5050 ESTABLISHED TCP 217.219.223.21:2031 63.121.106.74:80 TIME_WAIT TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING *:* UDP 64.110.148.59:138 *:* UDP 64.110.148.59:137 *:* UDP 64.110.148.59:9 *:* UDP 0.0.0.0:1958 *:*خب ميبينيد كه پورتهاي باز روي سيستم من ليست شده است. مثل 1954-1971-2031 دستور : Netstat -a اين دستور نيز مثل دستور Netstat -an يا Netstat -na عمل ميكنه فقط فرقش در اينه كه اين دستور پورتها را با معادل اسميشان نشان ميدهد ، براي مثال پورت 139 را با معادل اسميش يعني Netbiosنشان ميدهد و همچنين مانند دستور Netstat اسم صاحب سيستم را پرينت ميكند .(اين دستور براي تست كردن نقطه ضعفها و پورتهاي باز در سيستم هاي خودمان بسيار مفيد ميباشد و اگر سيستم آلوده به تروجن بود ميشود از اين دستورها و كلاً برنامه Netstatاين موضوع را فهميد ، پس آنهايي كه سوال ميكنند ما چگونه بفهميم سيستم خودمان آلوده به تروجن هست يا نه ، استفاده از اين دستور و كلاً دستورات Netstat ميتواند خيلي به آنها كمک كند ) دستور : Netstat -p xxx منظور از xxx يعني آن پروتكلي كه شما در نظر داريد كه ميتواند TCP و UDP باشد. دستور : Netstat -e اين دستور نيز يكي از دستورات Netstat است كه آماري از ارتباطها و بسته ها و شماره هاي ارسال و ذخيره بسته ها و داده ها را نشان ميدهد .(اين دستور بيشتر براي ويندوزهاي 98 me , و همينطور مودمهايي كه آمار بسته ها را نميدهند خوب و مفيد است چون در ويندوز 2000 -XP – قسمتي از اين آمار براحتي در اختيار User قرار ميگيرد ، و شما ميتونيد با استفاده از اين دستور ترافيک ISP و شبكه را ببينيد و همينطور برنامه هايي كه در حال دانلود هستسد را چک كنيد و يا اگر بسته اي در ارسالش مشكلي پيش بياد ميتوانيد در قسمت Errors مشاهده كنيد ، ...) دستور : Netstat -r اين دستور توسط كاربران معمولي اينترنت زياد بكار گرفته نميشود چون درک بعضي از گزينه هاش براي كاربران عادي دشوار ، بحرحال اين دستور جزييات دقيقي مثل آدرس ... , Gateway - Interface Metric -Netmask درباره آدرس آي پي شما در شبكه ميدهد ، همچنين در ويندوزهاي8 - 9 MEكار دستور Netstat -a را هم انجام ميدهد

گردآوری:

M93