آموزش ویندوز ۸ قسمت ۱۶ : ۱۰ دستور مهم در شبکه (نسخه PDF)

با جلسه ای دیگر از مجموعه آموزش های دوره MCSA مایکروسافت در خدمت شما عزیزان هستم. در جلسه پیش به نحوه راه اندازی یک شبکه ساده در ویندوز ۸ پرداختیم. در این جلسه اما قصد داریم تا شما را با یک سری دستورات مهم وکاربردی شبکه در ویندوز ۸ آشنا کنیم. این جلسه را شاید اگر مهمترین در سری مباحث دوره MCSA ندانیم، اما بی شک یکی از پر اهمیت ترین ها خواهد بود، چرا که مفاد این جلسه حتی در دوره های بعـدی ویـنـدوز سـرور نیز به کار خواهد آمد. پس در ادامه نیز با ما باشـید.نکته: فرض مـا در این آموزش بر این خواهد بود که شـما از قبل دو کامپیوتر را با یکدیگر شـبکه کرده باشید، و نیز به هر دوی آن ها دسترسی اینترنت داشته باشند، و اکنون به واسطه فرمان ها و ابزارهای گنجانده شده در ویندوز ۸ صرفا قصد عیب یابی و نیز آنالیز شبکه را داریم.

ipconfig

شروع آموزش امروز با دستور ipconfig می باشد. از این دسـتور به منظور مشاهده تنظیمات فعلی شـبکه هم چون IPهای استفاده شده بر روی کامپیوتر، DNSهـا و موارد مشـابه دیگر اسـتفاده می گردد. پس به واسـطه این دسـتور افراد قـادر به مشاهـده تنظیمات IP بر روی کامپیوترشان هسـتند. دسـتور دارای سوییـچ هایی نیز می باشـد که از ذکر آن ها چشم پوشـی می نماییم. در زیر می توانید خروجی اجرا شده این فرمان را در محیط PowerShell مشاهده کنید:

توضیحات:

۱- بیانگر IP های تنظیم شـده (Set) کـارت شـبکه ای با نام Ethernet Local Area Connection می باشـد، که در حال حاضـر قطع (Media disconnected) می باشد

۲- بیـانگر IP هـای تنظیم شـده کـارت شـبکه ای دیگر با نام Ethernet ۲ می باشـد، که این کـارت شـبکه نیز در حـال حاضـر قطع (Media disconnected) می باشد

۳- بیانگر IP های تنظیم شده کارت شبکه ای با نام Ethernet می باشد، که در حال حاضر وصل و دارای آی پی ۱۹۲.۱۶۸.۰.۱۰۴ می باشد

ping

Ping اختصار سـر واژگان Packet INternet Groper است، و از آن به منظور بررسـی وضـعیت ارتباطی دسـتگاه ها و کامپیوترها در شـبکه و اینترنت با یکدیگر استفاده می گردد.الگوریتم کارکرد این دستور نیز بدین صورت است که ping با ارسال بسته هایی به سمت سایت، سرور، یا کلاینت، منتظر پاسخ از سمت آن ها می ماند، و در صورت پاسخ دهی دستگاه مقصد، جواب را به ما برگشت خواهد داد. نحوه استفاده صحیـح از این فرمان، تایپ عبارت ping در PowerShell و سـپس آی پی یا نام کامپیوتر یا سایت مقصـد می باشـد. در زیر نیز می توانید فرمان اجرا شده به همراه جزییات آن را ببینید.

توضیحات:

۱- کامپیوتر ما با استفاده از ping بسته هایی را به مقصدی با آی پی ۱۹۲.۱۶۸.۰.۱ که نشانی یکی از کامپیوترهای شبکه مان می باشد ارسال کرده است.

۲- کامپیوتر هدف یا همان مقصد (۱۹۲.۱۶۸.۰.۱) درخواست ما را دریافت، و سـپس جواب را در قالب بسته های ۳۲ بایتی و در مدت زمان یک میلی ثانیه به ما برگشت داده، که نشان از برقراری ارتباط با مقصد دارد.

۳- گزارشـی از آن چه که انجـام شـده به ما برگشت داده می شود. در تصویر بالا تعـداد بسـته های ارسالی از سـمت ما چهار، بسـته های بازگشتی چهار، بسـته های از دست رفته که ممکن است به دلیل اختلال یا قطعی ناگهانی شـبکه در طول مسـیر رخ داده باشد صـفر، و در نهایت میانگین زمان انجام شده پروسه (Average)، صفر میلی ثانیه را نشان می دهد.

- نکته: در تصویر بالا TTL=۶۴ معرف نوع دستگاه یا سیستم عامل مقصدی می باشد که ping بر روی آن فرستاده شده است. گفتنی ست در مثال بالا عدد ۶۴ معرف یکی از نسخه های سیستم عامل مایکروسافت از خانواده NT (ویندوز ۱۰) می باشد. پس به واسطه مقدار TTL نیز می توان به نوع سیستم عامل یا دستگاه هدف پی برد. ضمن این که این مقدار برای دیگر دستگاه ها و سیستم عامل ها می تواند متفاوت از یکدیگر باشد. به عنوان نمونه این مقدار برای لینوکس ۶۴، یا مودم و روترهای موجود در شبکه ارقام دیگری هستند. برای درک بهتر نیز، در زیر مقدارهای گوناگون و این که هر کدام مربوط به چه دستگاه یا سیستم عامل هایی هستند آورده شده است:

Windows XP= ۱۲۸

Windows Server ۲۰۰۳= ۱۲۸

Windows Vista= ۱۲۸

Windows Seven= ۱۲۸

Windows Server ۲۰۰۸= ۱۲۸

Windows ۸= ۱۲۸

Windows ۱۰= ۶۴

Linux (Kernel ۲.۴ and ۲.۶)= ۶۴

Free BSD= ۶۴

Cisco Devices= ۲۵۵

توجه داشته باشید که در مثال بالا ما از ping به منظور وضعیت ارتباطی خودمان با IP یکی از کامپیوترهای شبکه مان استفاده کردیم، و این در حالی ست که می توان از ping به منظور وضعیت ارتباطی مان با وبسایت های اینترنتی نیز بهره ببریم، که در این صورت درخواست ما به سمت وب سایت اینترنتی ارجاع داده می شود، یعنی به جای استفاده از ip هر یک کامپیوترهای شبکه، این بار از نام سایت استفاده می کنیم: ping www.google.com

tracert

از این دستور به منظور بررسی وضعیت روترها یا سرورهای بین راه بسته اطلاعاتی، تا رسیدن به مقصد استفاده می گردد. تنها با این تفاوت که مدت زمان پاسخ دهی هر روتر و یا سرور نیز به میلی ثانیه به ما نمایش داده خواهد شد. این موضوع در بحث عیب یابی می تواند به ما کمک شایانی نماید، به خصوص در زمان هایی که شبکه مان به دلایل مختلف با کندی سرعت یا قطعی مواجه گشته، که با این تفاسیر می توانیم با بررسی مدت زمان پاسخ دهی هر یک از روترها یا سرورهای میان راهی از وضعیت آن ها نیز مطلع گردیم. به عنوان نمونه با اجرای این فرمان و چک کردن مدت زمان پاسخ دهی، اگر مقدار برگشتی از زمان معمول و متداول همیشگی بیشتر باشد، بایستی اقدامات بعدی را جهت عیب یابی انجام داد. در مثال زیر می توانید اجرا شده این فرمان را که در هر آدرس، و مدت زمان پاسخ هر دستگاه به میلی ثانیه را ببینید:

pathping

این دستور را باید ترکیبی از دو دستور بالا (ping و tracert) دانست. بدین صورت که pathping با ارسال بسته های اطلاعاتی به یک مقصد خاص، هم وضعیت برقراری ارتباط و احیانا قطعی آن را برایمان مشخص خواهد کرد، و هم مدت زمان پاسخ دهی دستگاه مقصد را محاسبه و نمایش می دهد. از این فرمان به خصوص برای زمان هایی که قصد عیب یابی دقیق تر شبکه را به همراه جزییات فنی بیشتر داریم استفاده می گردد. در زیر نیز می توانید اجرا شده این فرمان را به همراه توضیحات مشاهده کنید:

۱- ابتدا با اجرای فرمان pathping www.microsoft.com شروع به تست ارتباط با سایت مایکروسافت کرده ایم. درخواست تا رسیدن به سایت مایکروسافت از ۶ روتر عبور کرده است.

۲- در گزارشی که در پایان اجرای این دستور به ما داده شده است، مدت زمان میانگین رفت و برگشت در طول مسیر و بررسی تمام روترهای میان راهی۱۲۵ ثانیه به طول انجامیده.

۳- در سومین مسیر عبور بسته، که اگر خود کامپیوترمان را نیز به حساب بیاوریم در چهارمین مسیر عبور بسته خواهد شد، یک قطعی موقت رخ داده است. آی پی روتر یا سروری که این قطعی موقت در آن ایجاد شده ۱۹۲.۱۶۸.۱۱.۲ می باشد. اگرچه این قطعی می تواند به دلایلی هم چون وجود فایروال بر روی آی پی مذکور (۱۹۲.۱۶۸.۱۱.۲) یا پالیسی های خاص بر روی آن سرور نیز باشد.

nslookup

از این فرمان معمولا برای کشف IP سایت یا کامپیوترهای مختلف شبکه استفاده می شود. بدین صورت که پس از تایپ فرمان، و متعاقبا تایپ نام کامپیوتر یا سایت، IP آن برایمان نمایش داده خواهد شد. این دستور نیز می تواند در عیب یابی صحت کارکرد DNS Server شبکه که وظیفه تبدیل نام سایت به آی پی و بالعکس را دارد کمک شایانی نماید. مبحث DNS Serverها خود جلسه ای جداگانه را می طلبد که در این آموزش کوتاه نمی گنجد و در دوره های بعدی ویندوز سرور به آن می پردازیم. گرچه برای درک بهتر مفهوم DNS Server می توانید به مقالاتی که در همین زمینه در این وبسایت و نیز دیگر منابع اینترنتی موجود هستند مراجعه نمایید. در مثالی که در زیر و بر روی وب سایت www.sanjesh.org انجام شده، مشاهده می کنید که DNS سروری که کامپیوتر من از آن استفاده می کند، دارای آی پی ۱۹۲.۱۶۸.۱.۱ است که در این جا همان آی پی مودمم می باشد، و در ادامه نیز می بینید که آی پی برگشت داده شده سایت مذکور (سنجش)، ۹۲.۲۴۲.۱۹۵.۴ می باشد. پس از این که IP سایت کشف شد، می توان از آن نیز برای باز کردن سایت استفاده کرد.

netstat

netstat اختصار سر واژگان network statistics می باشد، و به منظور مشاهده وضعیت ارتباطات کامپیوتر با دنیای خارج استفاده می گردد. به واسطه این فرمان قادر خواهیم بود تا پورت های باز بر روی کامپیوترمان که با آدرس های خارجی هم چون اینترنت در ارتباط هستند را مشاهده کنیم. در واقع این دستور کلیه ی ورودی ها و خروجی ها به کامپیوتر شما را کنترل و بررسی می کند. netstat اطلاعات دیگری هم چون اتصالات و ارتباطاتی که از طریق هر کارت شبکه برقرار شده، و موارد دیگری را نیز به ما نشان خواهد داد.

به عنوان نمونه می توانید پورت هایی که بر روی کامپیوترتان در حالت Listening (انتظار برای برقراری ارتباط) و یاEstablished (ارتباط برقرار شده) هستند را مشاهده نمایید. این موضوع در عمل باعث خواهد شد تا اگر پورتی که نباید در حالت عادی بر روی کامپیوتر باز باشد را کشف نمایید که در عمل ممکن است با موارد مشکوکی نیز برخورد کنیم، موارد مشکوکی هم چون برنامه ای خاص که بر روی کامپیوتر و بدون این که از قبل توسط شما یا خود ویندوز تعریف شده باشد، اقدام به برقراری ارتباط با یک آدرس بیگانه خارجی نموده باشد، که گاها ممکن است نشان از وجود برنامه های جاسوسی بر روی کامپیوترمان داشته باشد.

در یک مثال می توان از برنامه جاسوسی Sub۷ نام برد، که با اجرا شدنش بر روی کامپیوتر به طور مخفیانه پورت شماره ۲۷۳۷۴ را که در حالت عادی به هیچ وجه نباید باز باشد را باز می کند و از آن برای خارج کردن اطلاعات شخصی تان بهره خواهد برد. در نتیجه در این مثال می بینیم که اگر پورت شماره ۲۷۳۷۴ که پورت مورد استفاده برنامه Sub۷ است، بدون اجازه ما باز شده باشد، سریعا بایستی اقدام به بستن آن از طریق فایروال نماییم. به مثالی دیگر در این زمینه توجه کنید:

ابتدا از طریق یک مرورگر اینترنتی وبسایت گوگل را باز کنید، و سپس با تایپ دستور netstat –n در PowerShell به نتایج زیر خواهیم رسید:

• این مثال بالا، ستون اول پروتکل هایی که شبکه مان در حال استفاده از آن ها می باشد نمایش داده شده است، که در این جا جنس تمام آن ها، پروتکل TCP هستند.

• ستون دوم شامل local address ها یا آدرس های محلی و نیز شماره پورت هایی ست که در حال حاضر کامپیوترمان از آن ها برای انتقال اطلاعات به دنیای خارج استفاده می کند. ضمن این که در این مثال تمام آدرس ها تنها اشاره به آدرس کامپیوتر من دارند.

• ستون سوم foreign address ها یعنی آدرس های خارجی و نیز شماره پورت هایی هستند که کامپیوتر من در حال ارسال داده بر روی آن

ستون سوم Foreign Address که یعنی آدرس کلی خارجی و نیز شماره پورت کلی متصل به کامپیوتر من در حال نرمش state بر روی آن ها می باشد. گفتنی ست که این آدرس ها و شماره پورت ها هم می توانند IPها و Portهای شبکه داخلی مان باشند، و هم IPها و Portهای شبکه خارجی هم چون اینترنت.

• و در نهایت ستون آخر وضعیت ارتباط (state) را نشان می دهد که به طور کلی برخی از این ها شامل:

ESTABLISHED یعنی ارتباط با آدرس و پورت مربوطه مربوطه در حال حاضر به طور کامل برقرار است.

TIME-WAIT یعنی ارتباط با آدرس و پورت مربوطه قبلا برقرار شده و اطلاعاتی نیز با آن آدرس رد و بدل شده، و اکنون ارتباط با آن دیگر برقرار نیست

LISTENING یعنی ارتباط با آدرس مربوطه در صف انتظار قرار گرفته، و به محض برقراری به حالت

ESTABLISHED در خواهد آمد

برای واضح تر شدن موضوع نیز می توان به یکی از نتایج به دست آمده که هایلایت نیز شده است اشاره کرد: در این مثال ارتباطی از سمت کامپیوتر من (۱۹۲.۱۶۸.۰.۱۰۴) و بر روی یکی از پورت های آن به شماره ۵۵۰۴۰ که پورت مورد استفاده مرورگر گوگل کروم می باشد، با یک آی پی خارجی (۶۴.۲۳۳.۱۶۱.۱۴۷) و بر روی پورت شماره ۴۴۳ برقرار شده است (ESTABLISHED). پس با این تفاسیر متوجه می شویم که دیگر جای نگرانی نخواهد بود و این پورت توسط مرورگر گوگل کروم در حال استفاده می باشد. ضمن این که توجه داشته باشید در صورت مشاهده موارد مشکوک می توانید با جستجوی شماره پورت های مشکوک در اینترنت، آن ها را توسط فایروال نیز مسدود و بلوکه نمایید، تا از بروز خطرات احتمالی جلوگیری نماییم. آموزش فایروال و نحوه بستن پورت در آن را نیز می توانید در این لینک ببینید.

در این جا از توضیحات بیشتر مرتبط با این فرمان چشم گوشی می کنیم و آموزش را با فرمان های مهم دیگر شبکه ادامه خواهیم داد.

nbtstat

لازمه ی درک مفهوم دستورnbtstat ، ابتدا آشنایی با NETBIOS می باشد. از این رو در ابتدا به بررسی ساختار NETBIOS خواهیم پرداخت.

معرفی پروتکلNetBIOS

NetBIOS را با یک مثال ملموس از دنیای واقعی شروع می کنیم. سازمان ثبت احوال کشور را در نظر بگیرید، تشابه نام و نام خانوادگی و حتی در مواردی نام پدر در این سازمان امری عادی محسوب می شود.به عنوان مثال ممکن است شما بیش از چندین نفر با نام داریوش آریا در این سازمان پیدا کنید اما این نام جدای از این که به ظاهر شبیه به یکدیگر هستند، ولی دارای یک شماره خاص در شناسنامه و یا کد ملی متفاوت می باشند که آنها را از یکدیگر متمایز خواهد کرد.

از این رو اگر فرضا شما بخواهید در این سازمان به دنبال داریوش آریا بگردید باید حتما کد ملی یا شماره شناسنامه ی وی را نیز بدانید، تا بتوانید فرد اصلی و مورد نظرتان بدون تداخل با دیگر افراد هم نام یافت شود.عین این مطلب را نیز در دنیای شبکه برای ارتباط و فرستادن داده ها بین کامپیوتر ها داریم، یعنی به عنوان مثال یک کامپیوتر در یک شبکه ورک گروپ (workgroup) یا تحت دامین (domain) باید دارای نام منحصر به فردی باشد تا زمانی که برای تبادل داده و اطلاعات می خواهد در شبکه اعلام حضور کند، بتواند به وسیله ی نام اختصاصی اش این کار را انجام دهد، که این موضوع به واسطه پروتکل NetBIOS انجام می پذیرد.

NetBIOS یک پروتکل تقریبا قدیمی ست که دیگر همانند گذشته کار تحت شبکه ای خاصی انجام نمی دهد و تنها یک اسم برای سیستم شما در نظر می گیرد که از ۱۶ کاراکتر تشکیل می شود، و به واسطه این اسم کامپیوتر شما راحت تر قابل شناسایی در شبکه محلی خواهد بود. این سرویس را اولین بار شرکت IBM طراحی، و سپس Microsoft آن را برای استفاده در سیستم عامل های مبتنی بر شبکه های مایکروسافتی پذیرفت. البته لازم به ذکر است که این پروتکل بر پایه پروتکل TCP/IP عمل می کند و پیرو آن می باشد. از NetBIOS برای خطایابی اتصال بین دو کامپیوتری که در تلاشند تا از طریق این پروتکل با یکدیگر ارتباط برقرار کنند استفاده می گردد. اگر تا بدین جای توضیحات راجع به NetBIOS را درک کرده اید، اکنون به سراغ اصل مطلب، یعنی دستور nbstat می رویم.

از فرمان nbtstat به منظور مشخص نمودن وضعیت کارکرد پروتکل NetBIOS در ارتباط های مبتني بر TCP/IP استفاده می شود. nbtstat معمولا برای تشخیص مشکلات NetBIOS مورد استفاده قرار مي گيرد. ضمن این که این نکته را مد نظر داشته باشید از آن جا کهnbtstat تنها بر بر روی پروتکل NetBIOS کار مي کند و NetBIOS نیز پروتکل اختصاصی مایکروسافت می باشد، در نتیجه از آن تنها در سیستم های

مبتني بر ويندوز اسـتفاده می گردد.این دسـتور نیز مانند دیگر دسـتوراتی که در بالا مورد بررسی قرار دادیم، دارای سوئیچ هایی می باشد، اما از آن جا که این فرمان دیکر همانند گذشـته کاربردی نبوده و از آن اسـتفاده نمی شود، از این روی به شـرح جزییات آن نمی پردازیم و صرفا جهت معرفی کلی و اطلاع پیدا کردن از نام چنین دستوری در این آموزش آورده شد.

getmac

پیش از توضیح راجع به این دستور نیز، اجازه دهید تا ابتدا با مفهوم MAC در کارت شبکه و نیز دستگاه های همراه همچون گوشی و تبلت آشـنا شویم. MAC اختصـار سـر واژگان Media Access Control و به معنـای کنترل دسترسـی وسایـل ارتبـاطی ست. هر وسـیله یا دسـتگاه اسـتانداردی همچون کامپیوتر، گوشـی و کلن تمامی دسـتگاه هایی که قادر به ارتباط با شـبکه و اینترنت به صورت بی سیم (WiFi) باشند، دارای یک آدرس MAC منحصر به فرد نیز هستند. این آدرس از ۱۲ رقم تشـکیل شده که حاوی اعداد و حروف هستند و با علامت نیم خط (-) یا دو نقطه (:) از یکدیگر جدا می شوند.

هر دسـتگاه در شـبکه دارای یک آدرس MAC یکتـا و منحصـر به فرد خودش می باشـد. از آدرس MAC در موارد گوناگونی که شایـد بتوان مهمترین آن را فیلترینـگ بر اساس آدرس MAC دانست اسـتفاده می گردد. یعنی افراد به واسطه MAC Filtering قادر می شونـد تا تنها به دسـتگاه های خاص و از پیش تعیین شده ای اجازه دسترسـی به منابع شبکه شان و یا اینترنت را بدهند. با تمام این تفاسیر و مواردی که در بالا گفته شد، می توانیم با اجرای فرمان getmac بر روی کامپیوترمان آدرس MAC آن را به دست آورده و از آن در سناریوهایی که نیاز به ایجاد محدودیت دسترسـی در شـبکه مان داریم استفاده کنیم. بهترین مثالی که در این زمینه نیز می توان زد، استفاده از MAC Filtering در اکسـس پوینت های بی سـیم و شـبکه های وای فای می باشد، که قطعا شـما نیز با آن بارها مواجه شده اید. در مثال زیر با اجرای فرمان مذکور، آدرس MAC کامپیوتری را به دست آورده ایم که با رنگ قرمز نیزهایلایت شده است.

netsh

فرمان netsh از دیگر فرمان های کاربردی شـبکه می باشد، که از آن به منظور ایجاد تغییرات در پیکربندی های شبکه مان استفاده می کنیم. تمـام هر آن چه که در واقعیت می توان در محیط گرافیکی وینـدوز بر روی کارت شـبکه انجام دهیم، از طریق این فرمان نیز قابل اجراست. تنظیماتی هم چون تغییر IP سیستم، اتصال به شبکه، و ...

به مثال توجه کنید:

```
netsh interface ip set address name=Ethernet static ۱۰.۰.۰.۱۰ ۲۵۵.۲۵۵.۲۵۵.۰ ۱۰.۰.۰.۱
```

پس از اجرای فرمان فوق، IP کارت شبکه مان که در این جا نام آن Ethernet می باشد، بر روی حالت Static) Manually) قرار خواهد گرفت، و به آن آی پی ۱۰.۰.۰.۱۰ با Subnet Mask: ۲۵۵.۲۵۵.۲۵۵.۰ و نیز Gateway: ۱۰.۰.۰.۱ تخصیص داده خواهد شد.

telnet

آخرین دسـتوری که در این آموزش مورد بررسی قرار خواهد گرفت فرمان telnet است. از telnet به منظور متصل شدن به دستگاهی دیگر در شبکه های محلی یا اینترنت و اجرای فرامین (Commands) بر روی آن ها استفاده می گردد. یعنی هر فرمانی را که با ویندوز قادر به اجرای آن هستیم، به واسطه telnet و اتصال به دستگاه های دیگر نیز می توانیم بر روی آن ها اجرا نماییم. این دستور به خصوص زمانی استفاده می شود که دارای سرعت مطلوبی نباشیم، یعنی فرض کنید بخواهیم با سرعت ۵۶k مودم دایال آپ پوشه ای را بر روی سروری در آن سوی دنیا ایجاد یا حذف نماییم. گرچه پیش از استفاده از این فرمان بایستی توجه داشت که ابتدا آن را از بایستی بر روی ویندوز نصب و فعال نمایید. بدین منظور مراحل زیر را پیش خواهیم رفت:

به Control Panel رفته و بر روی Uninstall a program از قسمت Programs کلیک نمایید

در صفحه ای که برایمان باز خواهد شد، بر روی Turn Windows features on or off کلیک می نماییم (تصویر زیر)

و سـپس مطابق تصویر زیر، یکی از دو گزینه Telnet Server و یا Telnet Client را انتخاب می نماییم. بایستی دقت داشت که اگر بخواهیم به دیگران اجازه وصل شدن به کامپیوترمان در شـبکه یا اینترنت را بدهیم تا آن ها قادر به اجرای فرمان های خاصـی به وسیله PowerShell یا Command Prompt بر روی کامپیوترمان باشند می بایست Telnet Server را انتخاب و نصب نماییم، در حالی که اگر خودمان بخواهیم به کامپیوتری دیگر در شـبکه یا اینترنت وصل شویم، بایستی Telnet Client را انتخاب و نصب نماییم. در این مثال زیر چون من قصـد دارم تا به کامپیوتری دیگر در شبکه وصل شوم، در نتیجه Telnet Client را انتخاب می کنم و بر روی OK کلیک می نمایم تا فرایند نصب و نیز فعال سازی telnet آغاز گردد.

پس از اتمـام فراینـد نصب، پیغامی نیز مبنی بر موفقیت آمیز بودن عملیات به ما نشان داده خواهـد شـد، که با زدن Close آن را نادیده گرفته و می بندیم

پس از انجام مراحل بالا، درست همین مراحل را نیز بر روی کامپیوتری که قصد اتصال به آن را داریم نیز انجام دهید، تنها با این تفاوت که این بـار به جای telnet client، گزینه telnet server را بر روی انتخـاب و فعـال می کنیم.اکنون اگر تمـام مراحل بالا را با موفقیت انجام داده باشید، وقت آن رسیده تا با استفاده از telnet به سروری در شبکه و یا اینترنت متصل شویم، و پس از اتصال اقدام به اجرای فرامین بر روی آن کنید. در مثال زیر من به سرور سایتی با نام igormud.org و بر روی پورت شماره ۱۷۰۱ آن که باز می باشد telnet کرده ام:

و آن گونه که مشاهـده می کنید، سـرور مقصد از ما تقاضای نام کاربری و پسورد کرده است، که در صورت صـحیح وارد کردن نام کاربری و پسورد، اصـطلاحا بر روی آن سـرور لاگین خواهیم کرد و قادر به اجرای فرامین و دستورات مورد نظر بر روی آن خواهیم بود. و آن گونه که در شـکل زیر نیز مشاهده می نمایید، توانسته ام با استفاده از دستور telnet بر روی سرور سایت igormud.org و پورت شماره ۱۷۰۱ آن که باز می باشد لاگین نمایم، و این موضوع بدان معناست که از این پس قادر به اجرای دستورات بر روی این سرور خواهم بود.

امیدوارم آموزش این جلسه مورد توجه شما عزیزان قرار گرفته باشد.

با آرزوی شادی برای یکایک ایرانیان

نویسنده : اسحاق احمدپور

منبع : جزیره سرویس های شبکه مایکروسافت وب سایت توسینسو

karagah

ممنون واقعا

اسحاق احمدپور

Your welcome dear

Aryana_bd

خیلی ممنون

hesamazizi

خیلی ممنون.خسته نباشین

مطلب اصلی