E-mail: God.Hacked@Yahoo.com

Website: Www.Expolit.Net.Tf

ملاحضات:

با سلام از اینکه مقاله من را جهت اموزش انتخاب کردین سپاس گزارم. اما کاربر گرامی این مقالات فقط جهت اموزش نوشته شده و در اختیار شما قرار گزاشته شده و هر گونه استفاده غیر اموزشی از ان بر عهده خود کاربر میباشد و اینجانب هیچ گونه مسئولیتی بر عهده نمیگیرم. با تشکر: پیام ایزدی.

((صحبت با پرتها))

اولين نكته‌ي كه بايد بگم اين است كه ابزاري كه به كمک آن با پورت‌ها صحبت مي‌كنيم در همه پورت‌ها يكي است ولي هر پورتي زبان مخصوص خود دارد (درست مثل زبان‌هي مختلف در جهان كه همشون از طريق زبان و دهان ادا مي‌شن ولي هر كدام روش خاصي بري ارتباط برقرار كردن دارند). پس ما بري كار با پورت‌ها بايد زبان هركدام را ياد بگيريم.

بحث بعدي اين است كه وقتي مي‌گيم يه پورت بازه بايد توجه كنيد كه برنامه‌ي روي آن كامپيوتر نصب شده و اون پورت را باز كرده است (پورت‌ها خود به خود باز نمي‌شوند). يک سري پورت‌ها توسط خود سيستم‌عامل باز مي‌شوند (يعني به محض نصب سيستم‌عامل كه خودش هم درواقع يه نرم‌افزاره) و نيازي نيست كه برنامه ديگري برايش نصب كنيم. در مقابل، بعضي پورت‌هي ديگر توسط برنامه‌هي جانبي باز مي‌شوند.

به عنوان مثال وقتي مي‌گم كه پورت ۲۵ روي يک ip باز است، اين معني را دارد كه برنامه‌ي روي اون كامپيوتر خاص وجود دارد كه پورت ۲۵ را باز كرده و من وقتي از طريق كامپيوتر خودم با آن پورت كار مي‌كنم در واقع دارم با آن برنامه خاص (كه اون پورت را باز كرده) صحبت مي‌كنم.

حالا يه سوال پيش مي‌آد كه چرا اصلا يه نرم‌افزار بايد پورت باز كنه و اينكه كدام نرم‌افزارها بايد پورت باز

کنند؟
جواب این است که هر برنامه‌ي که بخواهد از طریق شبکه (یعني از راه دور اصطلاحا remote) قابل دسترس باشه باید یه پورت باز کنه. پس یک برنامه‌ي که نیازي به برقراري ارتباط شبکه‌ي ندارد (مثلا یه نرم‌افزار گرافیکي) نباید و نشاید که پورت باز کند.

باید ببینیم که از طریق چه برنامه‌ي مي‌توان با پورت‌ها صحبت کرد (البته با هرکدام به روش خودشان)؟
بري این‌کار از دو نرم‌افزار به نام‌هي telnet و nc استفاده مي‌کنیم. telnet که در خود سیستم‌عامل وجود دارد و nc را هم که جلسه قبل داون‌لود کردیم.
حالا چگونه از این دو نرم‌افزارها مي‌توان استفاده کنیم؟
۱- استفاده از telnet :
اگر بخواهیم با ip ي به شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ از طریق پورت ۲٥ صحبت کنیم باید بنویسیم:

telnet 194.225.184.13 25

و بعد اینکه ارتباط برقرار شد باید شروع کنیم و از طریق زبان پورت ۲٥ با آن صحبت کنیم.
۲- استفاده از nc :
اگر بخواهیم همان کار را با netcat انجام دهیم، باید بنویسیم:

۲٥ ۱۹٤,۲۲٥,۱۸٤,۱۳ nc -v

و بعد از برقراري ارتباط شروع به صحبت کنیم.

◊ با پورت ۱۳ صحبت کنیم

نام دیگر اون daytime است و کارش هم اینه که زمان و تاریخ رو در اون کامپیوتر به ما مي‌ده. این پورت اصولا خیلي سر راسته. فقط کافیه که بهش وصل شیم تا اطلاعاتشون بیرون بریزه. البته این پورت رو خیلي از کامپیوترها بسته است. (یادتون باشه که وقتي مي‌توان با یه پورت کار کرد که باز باشد).
حالا مي‌خوایم با پورت ۱۳ از ip شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ صحبت کنم. یکي از این دو دستور را مي‌نویسم:

telnet 194.225.184.13 13
۱۳ ۱۹٤,۲۲٥,۱۸٤,۱۳ nc -v

البته در آن دستورات به جي عدد ۱۳ مي‌توان معادلش را نوشت که daytime است.
و جواب مي‌شنوم:

AM 10/5/2002 ۱۱:۳٥:۳۳

بله، با این پورت ارتباط برقرار کردیم و اطلاعاتش رو دریافت کردیم. این اطلاعات معمولا به درد این مي‌خورد که مکان جغرافیایي اون کامپیوتر را حدس بزنیم (البته اگر زمان اون کامپیوتر صحیح باشد). به عنوان مثال این کامپیوتر خاص در ایران است چون ساعتش همزمان با ایران است.

◊ با پورت ۷ صحبت کنیم

اسم این پورت echo است. من این پورت رو پورت میمون مي‌گم چون هرچي که شما براش بنویسید را تقلید مي‌کنه و همان‌ها را براتون پس مي‌فرستد. مثلا من به پورت ۷ کامپیوتري با ip شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ تلنت یا nc مي‌کنم.

telnet 194.225.184.13 7
۷ ۱۹٤,۲۲٥,۱۸٤,۱۳ nc -v

بعد از برقراري ارتباط، هر چي من بنويسم، اون برام پس مي‌فرسته. مثلا اگه تايپ كنم Ali1000 و Enter بزنيم، جواب مي‌شنوم، Ali1000 ... خودتون امتحان كنيد تا ببينيد. بري تمام شدن كار بايد دكمه Ctrl+C را فشار دهيم تا اين ميمون بازي تموم بشه.
پس كار كردن با اين پورت هم زياد سخت نيست.

پورت ۸۰ چيست؟ϖ

پورت ۸۰ يكي از مهم‌ترين پورت‌هاست. دنيي وب (صفحات اينترنتي) بر اساس همين پورت كار مي‌كنه. توضيح اينكه وقتي به يه سايت وصل مي‌شيم و صفحه وب را درخواست مي‌كنيم، در واقع مرورگر اينترنتي به پورت ۸۰ اون كامپيوتر وصل مي‌شه و اطلاعات رو مي‌گيره (البته بعد از گرفتن اطلاعات اون رو تفسير مي‌كنه و به صورت يه صفحه نشون مي‌ده - دقت كنيد كه اطلاعات در واقع به صورت يک سري تگ HTML است).

با پورت ۸۰ صحبت كنيمϖ

حالا ما مي‌خواهيم با پورت ۸۰ يک كامپيوتر صحبت كنيم ولي به كمک telnet و nc.
اول بايد يه connection (اتصال) با پورت ۸۰ برقرار كنيم (مثلا بري سايت hotmail.com بايد بنويسم):
telnet www.hotmail.com 80

nc -v www.hotmail.com 80
پس اول بايد يكي از دستورات بالا را استفاده كنيم. من هميشه توصيه‌ام استفاده از nc بوده و خواهد بود.
حالا بايد شروع به صحبت با پورت ۸۰ كنيم. من فعلا دو تا جمله براتون مي‌گم و بقيه‌اش بمونه واسه بعد. دقت كنيد كه موقع كار با پورت ۸۰ با تلنت (نه nc) دستوراتي كه ما مي‌نويسيم، نمايش داده نمي‌شود ولي كار مي‌كنه.
۱- اولين جمله اينه: GET / HTTP/1.0 و بعدش دوتا Enter
به فاصله‌ها دقت كنيد. دو طرف / ي كه بعد از GET است، فاصله وجود دارد. اين جمله به پورت ۸۰ مي‌گه كه هرچي در header داره، نشون بده. و جواب مي‌شنوم:
Temporarily HTTP/1.0 302 Moved

Server: Microsoft-IIS/5.0

GMT ۱۲:۰۲:۵۱ ۲۰۰۲ Date: Thu, 05 Dec

http://lc2.law5.hotmail.passport.com/cgi-bin/login :Location

cache5.neda.net.ir X-Cache: MISS from

Connection: close

۲- دومين جمله اينه: what/ever / GET و بعدش دوتا Enter
به فاصله‌ها دقت كنيد. اين دستور باعث ميشه كه هر چي داره، رو كنه.

البته توجه كنيد كه ما مسير را مشخص نكرديم. اين حالت كه بدون مسير است خيلي وقت‌ها كار نمي‌كنه (مثل همين مثال !!)

گاهي پيش مي‌آد كه يک سري دستورات خاص را هميشه بايد پشت سرهم به يه پورت خاص بفرستيم و بخواهيم در وقت صرفه‌جويي كنيم. مثلا همين جمله GET / HTTP/1.0 و دو Enter پشت سرهم كه هميشه استفاده مي‌كنيم. در اين موارد مي‌توان اين دستورات را در يک فايل تايپ كرد (همراه با Enter ها كه بايد موقع نوشتن حتما بزنيد) و بعد مثلا با نام ali.txt ذخيره كنيد و بعد يكي از دستورات زير را بنويسيم:

```
ali.txt > nc -v www.far30.com 80
```

```
type ali.txt | nc -v www.far30.com 80
```

كه همان كارهي بالايي را انجام ميده.

حالا مي‌خوام مسير رو مشخص كنمϖ

مثلا فرض كنيد كه مي‌خوام فايلي به اسم index.html را از مسير startup در سايتي به اسم www.site.com داون‌لود كنيم. اول يه nc مي‌كنيم به سايت. بعد مي‌نويسيم:

```
startup/index.html HTTP/1.0/ GET
```

بعد دو تا Enter مي‌زنيم.
اين مثال نشون ميده كه چطوري مسير رو ميشه مشخص كرد. همين كار رو مي‌تونيم براي فايل‌هايي مثل فايل‌هاي گرافيكي و ... انجام بديم و حتي مي‌تونيد اطلاعاتي كه مي‌رسه رو در يک فايل ذخيره كنيد. براي اين‌كار مي‌نويسيد:

```
index.html < nc -v www.site.com 80
```

(اين كاري كه كرديم با موردي كه در بالا نوشتيم فرق مي‌كنه! در بالا دستورات GET رو تو يه فايل مي‌نوشتيم و مي‌فرستاديم كه اجرا بشه ولي الان داريم نتايجي كه بر مي‌گرده رو در يک فايل ذخيره مي‌كنيم!) ميشه اين دوتا رو تركيب كرد مثلا نوشت:

```
index.html < dastoorat.txt > www.site.com 80 nc -v
```

پورت ۷۹ چيست؟

پورت ۷۹ را پورت finger مي‌گويند. كاربرد اين پورت به اوايل ايجاد اينترنت برمي‌گرده و كاربردش مخصوص سيستم‌عامل يونيكس بوده‌است (الان هم تقريبا فقط در خانواده سيستم‌هي يونيكس اين پورت قابل استفاده است).
وقتي اين پورت روي سيستم‌عامل يونيكس باز باشه، مي‌شه با يک request ساده فهميد كه از بين كساني كه در آن سيستم account دارند، كدام‌ها on هستند (يعني كدام‌ها به سيستم login شده‌اند). برنامه‌اي كه پورت ۷۹ رو در يک سيستم باز مي‌كنه، finger server مي‌گن و چون مختص سيستم‌عامل يونيكس است، مي‌تونين از عبارت Finger Deamon استفاده كنين. حالا كه پورت ۷۹ روي سيستم باز شد، شما مي‌تونين با اون ارتباط برقرار كنين.

با پورت ۷۹ صحبت كنيمϖ

همان‌طور كه مي‌دانيد، براي صحبت كردن با پورت‌ها از دو برنامه telnet و nc ميشه استفاده كرد. در مورد پورت ۷۹ يه نرم‌افزار ديگر به نام finger در تمام سيستم‌عامل‌هي يونيكس و برخي سيستم‌عامل‌هاي ويندوز وجود دارد كه علاوه بر دو برنامه قبلي، اونم مي‌شه به كار برد.
فرض كنيد كه مي‌خوام با پورت ۷۹ در كامپيوتري به اسم router2.iums.ac.ir ارتباط برقرا كنم. بري اين كار يكي از سه دستور زير را استفاده مي‌كنم:

```
router2.iums.ac.ir 79 telnet
nc -v router2.iums.ac.ir 79
router2.iums.ac.ir@. finger
```

دقت كنيد كه در دو دستور اول شماره پورت مشخص شده ولي دستور آخري نه، چون دستور finger فقط براي همين‌كار استفاده مي‌شه و نمي‌توان باهاش با پورت ديگه‌ي ارتباط برقرار كرد. ضمنا به ساختار دستور آخر توجه كنيد. بعد از اجري دستور، جواب مي‌شنوم:

```
Line User Host(s) Idle Location
```

Async interface 0 tty 33 whgh ٣٣
tty 34 najahan Async interface 0 ٣٤
interface 0 tty 35 sadf Async ٣٥
tty 36 abokho Async interface 0 ٣٦
interface 0 tty 38 whgh Async ٣٨
tty 39 bzamani Async interface 0 ٣٩
interface 0 tty 40 saeedmah Async ٤٠
tty 41 mfaizi Async interface 0 ٤١
interface 0 tty 42 gourabi Async ٤٢
tty 43 farhadz Async interface 0 ٤٣
interface 0 tty 44 arbks Async ٤٤
tty 45 mhalavi Async interface 0 ٤٥
interface 0 tty 46 farhood Async ٤٦
tty 47 staavoni Async interface 0 ٤٧
interface 0 tty 48 whgh Async ٤٨
vty 0 idle 0 217.218.84.58 ٦٦ *

Peer Address Interface User Mode Idle
نكته مهم اين است كه اطلاعاتي كه به كمک پورت ٧٩ به دست مي‌آد، خيلي بستگي به سروري داره كه اين اطلاعات رو مي‌فرسته. بعضي از سيستم‌ها علاوه بر نام افراد (username) كه در اين مثال ديده مي‌شه، نام و نام خانوادگي افراد، ساعت و محل login كردن و ... را نمايش مي‌دهند. اما چيزي كه هميشه وجود دارد و مشترک است، username هاست كه از نقطه نظر يک هکر بسيار ارزشمند است. در اين مثال ما اكانت‌هايي به اسم whgh،najahan و ... در اين سرور وجود دارد و افراد مربوطه در حال حاضر login كرده‌اند. اگر اكانتي موجود باشد ولي فرد مورد نظر در حال حاضر از آن اكانت وارد نشده باشد، نمايش داده نمي‌شود. اين ليست فقط براي اكانت‌هي فعال است. پس نتايجي كه شما در ارتباط با اين سرور كسب مي‌كنيد، با نتايجي كه من نوشتم متفاوت خواهد بود.

اين اطلاعات به چه دردي مي‌خورد؟ϖ

اول اينو بگم كه finger كردن، جزئي از مراحل Enumeration است (البته در حالت كاربرد legal يا قانوني). منظور از عبارت Enumeration يا به طور خلاصه Enum، پيدا كردن ليست كاربران است.
+ فرض كنيد مي‌خواهيد يک ليست از پسوردها را تست كنيد تا اينكه يكي شانسي درست در بياد (درست مثل دزدها كه يه سري كليد را تست مي‌كنن كه يكي به قفل بخوره و باز كنه!) حالا سوال اينه كه اين پسوردها رو بري چه username ي تست مي‌كنيد؟ جواب، username هايي است كه با Enumeration به دست اومده است. پس اول با Enumeration يه ليست پيدا مي‌كنيد و بعد تعداد زيادي پسورد رو روش تست مي‌كنيد (روش اين كارو بعدا مي‌گم).
+ كاربرد بعدي finger در رابطه با يک سري اكانت‌هاي خاص است. من هميشه وقتي به يک اكانت به اسم guest برخورد مي‌كنم، هميشه پسوردهي guest يا libguest يا myguest و ... رو تست مي‌كنم كه گاهي جواب ميده. همين‌طور در مورد اكانتي به اسم demo پسورد demo را تست مي‌كنم و ... معمولا موسسات بزرگ پر است از اين username هاي عمومي كه حدس زدن پسورد مربوطه كار مشكلي نيست.
+ گفتم كه بعضي سرورهاي finger نام و نام‌خانوادگي افراد را هم برايمان مي‌فرستند. چون بعضي از افراد متاسفانه يا خوشبختانه از اين اطلاعات براي پسوردشون استفاده مي‌كنند، مي‌تونه مفيد باشه.
+ يک كاربرد ديگه و البته بسيار مهم موقعي است كه مثلا مي‌خواهيد يک سري پسورد رو روي يک اكانت خاص تست كنيد. من هميشه اول يک finger مي‌كنم كه مطمئن بشم كه فرد در حال حاضر login نكرده باشد و بعد اين كار رو شروع مي‌كنم (يعني انقدر صبر مي‌كنم كه ديگه آن اسم خاص در finger نمايش داده نشه يعني طرف مقابل logout كرده باشد

پورت ٢١ چيست؟

پورت ٢١ رو پورت ftp مي‌گن. ftp مخفف عبارت file transfer protocol است يعني پروتكل انتقال فايل. كاربرد اين پروتكل و اين پورت از زماني وجود داره كه حتي وب (پورت ٨٠) هم چندان عمومي نشده

بود. پس مي‌تونم بگم كه يه پروتكل باستاني هستش. وقتي مي‌خواهيد با يک سرور از طريق اين پروتكل صحبت كنيد، بايد مطمئن بشين كه سرويس مربوط به ftp روي اون كامپيوتر فعال باشه. به عبارت ديگه بايد يک ftp server روي اون كامپيوتر در حال اجرا باشه. حالا شما با اون كامپيوتر مي‌خواين ارتباط برقرار كنين، پس شما بايد از يک ftp client استفاده كنيد. پس شما كلاينت هستيد و دستگاه مقابل سرور!
حالا شايد بپرسين كه كار ftp چيست؟
ftp براي انتقال فايل به كار ميره و اين انتقال فايل در دو جهت ممكنه كه upload و download گفته ميشه. براي اينكه اين‌ها رو قاطي نكنيد با هم فرض كنيد كه كامپيوتر سرور بالي سر شما قرار گرفته، پس وقتي فايل رو از اون مي‌گيريد، فايل به سمت پايين مي‌آد (download) و وقتي فايل رو براي سرور مي‌فرستيد، حالت برعكس مي‌باشد و بهش مي‌گيم، upload كردن. و هر دو عبارت نوعي انتقال فايل محسوب ميشه. دقت كنيد كه انتقال فايل از طريق پروتكل‌هاي ديگه‌اي هم امكان‌پذيره مثل web و ... ولي ما بحث‌مون همين پروتكل ftp است.
عبارت ديگه‌اي كه راجع به اين پورت بايد ياد بگيريد، عبارت anonymous است. براي توضيح اين عبارت اول بايد بگم كه وقتي شما مي‌خواهيد با سرور ارتباط برقرار كنيد، همين‌طوري كشكي كه نيس! براي ارتباط با سرور از شما username و password پرسيده مي‌شه و اگه درست باشه مي‌تونين فايل‌ها رو upload و download كنيد و تغيير بديد (پس مي‌بينيد كه اين پروتكل پروتكل حساسي است و اگه هک بشه خيلي كارها ميشه باهاش كرد). اين حالت كه گفتم در حالتي ممكنه كه شما username و password داشته باشيد. اما گاهي پيش مي‌آد كه username و password نداريم و مي‌خوايم با پورت ftp يک سرور يا سايت ارتباط برقرار كنيم. در اين حالت معمولا فقط اجازه download به ما داده ميشه و اجازه upload و يا اعمال تغييرات در فايل‌ها رو نداريم و اونو حالت anonymous يا ناشناس مي‌گن. در اين حالت وقتي از ما username خواسته ميشه، عبارت anonymous را تايپ مي‌كنيم و بعد كه پسورد پرسيده ميشه، شما بايد E-mail تون رو وارد كنيد، ولي من مي‌گم كه به جاي E-mail واقعي تون يه E-mail الكي بنويسين مثلا alaki@dolaki.com !!
آدرسي كه براي ftp با يه سرور استفاده مي‌كنيم به چه شكلي است؟
آدرسي كه استفاده مي‌كنيم بستگي به سرور داره ولي معمولا ساختار ثابتي داره. (اگه يادتون باشه واسه web مثلا مي‌نوشتيم، www.far30.com) حالا براي ftp مي‌نويسيم، ftp.far30.com پس مثلا براي سايت sazin.com مي‌نويسيم، ftp.sazin.com كه آدرس ftp سايت ميشه.

- چطوري يه سرور پيدا كنم كه سرويس ftp روي اون فعال باشه؟

اين سوال دو حالت داره:
۱- مي‌خواهيد به صورت anonymous وارد بشين يعني username و password نداريم. براي اين حالت مي‌تونين از خيلي از سايت‌ها استفاده كنيد. مثلا مي‌تونين از ftp.microsoft.com استفاده كنيد يا سايت‌هاي ديگه.
۲- اگه مي‌خواهد به صورت غير anonymous كار كنيد، حيطه عمل‌تون محدود به سايت‌هايي ميشه كه username و password واسه اون دارين. مثلا اگه شما سايتي روي اينترنت داشته باشيد (چه سايت پولي و چه سايت مجاني مثلا در netfirms و geocities و ...) به شما يک آدرس ftp و يک username و password تعلق مي‌گيره كه از طريق اون كار مي‌كنيد. اگه سايت نداريد، مي‌تونيد يک سايت مجاني درست كنيد. مثلا مي‌تونيد از سايت geocities.com كه متعلق به ياهو است استفاده كنيد. يا از سايت‌هي netfirms.com يا freeservers.com و... ولي به‌هر حال در يكي از اين‌ها ثبت‌نام كنيد و username و password بگيريد. آدرس‌هاي ftp آنها هم كه به‌صورت ftp.geocities.com يا ftp.netfirms.com و... خواهد بود. (از من نخواين كه طريقه ثبت‌نام در اين سايت‌ها رو هم به شما ياد بدم! كار خيلي راحتيه.)

- با پورت ۲۱ صحبت كنيم

فرض كنيد من از يک سايت فرضي استفاده مي‌كنم كه آدرس ftp اون باشه: ftp.somesite.com و username من باشه ali100• و پسوردم هم يه چيزه ديگه باشه. حالا مي‌خوام از طريق پورت ۲۱ با اين سايت ارتباط برقرار كنم. در مورد اين پورت ديگه از nc و telnet استفاده نمي‌كنم، بلكه از برنامه‌اي كه در تمام ويندوزها هست، به اسم ftp كمک مي‌گيرم. در command prompt مي‌نويسم:

```
ftp.somesite.com ftp
```

و جواب مي‌شنوم:

```
.Connected to somesite.com
.(somesite Microsoft FTP Service (Version 5.0 ۲۲۰
:((User (somesite.com:(none
```

دقت کنید که این سایت ftp server اش از نوع Microsoft است، پس این سرور از سیستم‌عامل ویندوز استفاده مي‌کنه (دونستن این نکات لازم نیست، ولي من توصیه مي‌کنم که همیشه به جزئیات توجه کنید) دقت کنید که از من username رو مي‌خواد، پس مي‌نویسم: ali1000 و Enter رو فشار مي‌دم. جواب مي‌آد:

```
.Password required for ali1000 ۳۳۱
:Password
```

حالا ازم پسورد مي‌خواد و پسورد رو تایپ مي‌کنم. جواب مي‌شنوم:

```
.User ali1000 logged in ۲۳۰
<ftp
```

این نشون میده که تونستم با پورت ۲۱ کامپیوتر مقابل ارتباط برقرار کرده و اصطلاحا یک session یا نشست! باهاش داشته باشم. اگه username یا password اشتباه بود، اون موقع مي‌گفت:

```
.User ali1000 cannot log in ۵۳۰
.Login failed
<ftp
```

من فرض مي‌کنم که session با موفقیت برقرار شده، حالا تایپ مي‌کنم:

<ftp **help**

و جواب مي‌شنوم:

```
:Commands are  .Commands may be abbreviated

send          prompt        literal        delete          !
              put           ls             debug           ?
                                                          status
trace         pwd           mdelete        dir             append
type          quit          mdir           disconnect      ascii
user          quote         mget           get             bell
              recv          mkdir          glob            binary
                                                          verbose
          remotehelp        mls            hash            bye
              rename        mput           help            cd
              rmdir         open           lcd             close
```

این‌ها لیست دستوراتي است که مي‌تونید استفاده کنید. من فقط اون‌هایي که به صورت bold مشخص کردم رو توضیح خواهم داد. بقیه دستورات کمتر به کار مي‌رن.

- دستورات پایه براي این پورت کدامند؟

+ دستور **help** و **?**
دستور help رو همین الان استفاده کردیم. دستور ? هم معادل اونه.

+ دستور **dir** و **ls**
این دو دستور نشون مي‌دن که در محل فعلي در سرور چه فایل‌ها و فولدر (دایرکتوري) هایي وجود دارد. فرق‌شون اینه که وقتي از dir استفاده مي‌کنید، اطلاعات بیشتري علاوه بر نام فایل‌ها و فولدرها به ما میده. من نوشتم **dir** و جواب شنیدم:

```
.PORT command successful ٢٠٠
.Opening ASCII mode data connection for /bin/ls ١٥٠
db          <DIR >      AM٠٢:١٨  ٠٢-٢٨-١٢
Special     <DIR >      AM٠٢:١٩  ٠٢-٢٨-١٢
www         <DIR >      AM٠٣:١٨  ٠٣-٠٨-٠٣
.Transfer complete ٢٢٦
.ftp: 135 bytes received in 0.02Seconds 6.75Kbytes/sec
```

ملاحظه مي‌فرماييد كه سه تا فولدر (دايركتوري) اينجا هست. (اگه با دستور dir آشنا نيستيد، يک كتاب داس بخونيد). اين‌ها فولدر هستند چون عبارت < DIR> جلوي اون‌ها نوشته شده است. نام اين فولدرها عبارتند از db و special و www

+ دستورات مرتبط با كار روي فولدرهايي كه روي سرور (نه روي كامپيوتر خودمون) هستند، عبارتند از:
cd يا **chdir** ==> اين دستور براي وارد شدن داخل يک فولدر به كار مي‌ره.
mkdir ==> اين دستور براي ساختن يک فولدر جديد به كار ميره.
rmdir ==> اين دستور براي پاک كردن يک فولدر موجود به كار ميره (به شرطي كه آن فولدر خالي باشد)
براي كار با هر كدوم از اين دستورات كافي است، دستور مورد نظر را نوشته و بعد از يک كاراكتر فاصله، نام فولدر را بنويسيد، مثلا اگه بخوام وارد فولدر www بشم، مي‌نويسم:

```
www cd
```

و جواب مي‌شنوم:

```
.CWD command successful ٢٥٠
<ftp
```

اين جواب به آن معني است كه وارد فولدر (دايركتوري) www شده‌ام. حالا دوباره دستور dir را استفاده مي‌كنم و جواب مي‌گيرم:

```
.PORT command successful ٢٠٠
.Opening ASCII mode data connection for /bin/ls ١٥٠
private_          <DIR >      AM٠٢:١٨  ٠٢-٢٨-١٢
jpg.١ ٦١٩٨٢                   PM٠٤:١٥  ٠٣-١٧-٠٢
aspnet_client     <DIR >      AM٠٢:١٩  ٠٢-٢٨-١٢
cgi-bin           <DIR >      AM٠٢:١٩  ٠٢-٢٨-١٢
default.asp ١١٢٨٥             PM٠٦:٢٧  ٠٢-٢٩-١٢
images            <DIR >      AM٠٢:١٩  ٠٢-٢٨-١٢
postinfo.html ٢٤٩٤            AM٠٢:١٨  ٠٢-٢٨-١٢
.Transfer complete ٢٢٦
.ftp: 1438 bytes received in 0.28Seconds 5.12Kbytes/sec
<ftp
```

ملاحظه مي‌كنيد كه سه تا فايل و سه تا دايركتوري داريم. اون‌هايي كه جلوشون نوشته < DIR> دايركتوري هستند و اونايي كه اين عبارت رو ندارند و جلوشون يه عدد نوشته شده (كه بيانگر حجم هر كدومشون هست) فايل مي‌باشند.
در مورد دستور cd اگه بنويسم **cd ..** به فولدر قبلي بر مي‌گرديم، مثلا الان كه تو فولدر www هستيم اگه .. cd رو بنويسم، يک فولدر به عقب برمي‌گردم (به حالت قبل از ورود به www)
يه دستور ديگه هم راجع به فولدرها هست و اونم دستور **pwd** است. اين دستور نشون ميده كه ما الان تو كدوم فولدر از فولدرهاي سرور هستيم.

+ دستورات مرتبط با فايل‌ها عبارتند از:
delete يا **dele** ==> اين دستور براي پاک كردن يک فايل به كار مي‌ره.
rename ==> اين دستور براي عوض كردن نام يک فايل به كار مي‌ره.
مثلا اگه بخوام فايل default.asp رو پاک كنم، مي‌نويسم **delete default.asp**
اگه بخوام فايل default.asp رو به index.htm تغيير نام بدم، مي‌نويسم **rename default.asp index.htm**

+ دستورات مرتبط با فولدرهاي كامپيوتر خودمان:
اول دقت كنيد كه در مورد پورت ۲۱ وقتي مي‌گوييم در كدام فولدر قرار داريم، اين مسئله دو معني داره. حالت اول محل فعلي ما روي سرور است. يعني كجاي سرور هستيم. تمام دستوراتي كه راجع به فولدرها گفتم براي كار روي فولدرهاي سرور است. حالت دوم محل فعلي ما در كامپيوتر خودمون است. فرض كنيد كه وارد فولدري در كامپيوتر سرور شده‌ايم والان مي‌خوايم فايل را داون‌لود كنيم به كامپيوتر خودمون. براي اينكه فايل به فولدر درستي در كامپيوتر خودمون منتقل بشه، بايد وارد يک فولدر خاص در كامپيوترمان بشيم. دستور مرتبط با اون دستور **lcd**است. مثلا اگه بخوام وارد فولدر araz از درايو C: بشم، مي‌نويسم:

```
c:/araz lcd
```

نويسنده: پيام ايزدی E-mail: God.Hacked@Yahoo.Com

The Hacking of God.Hacked