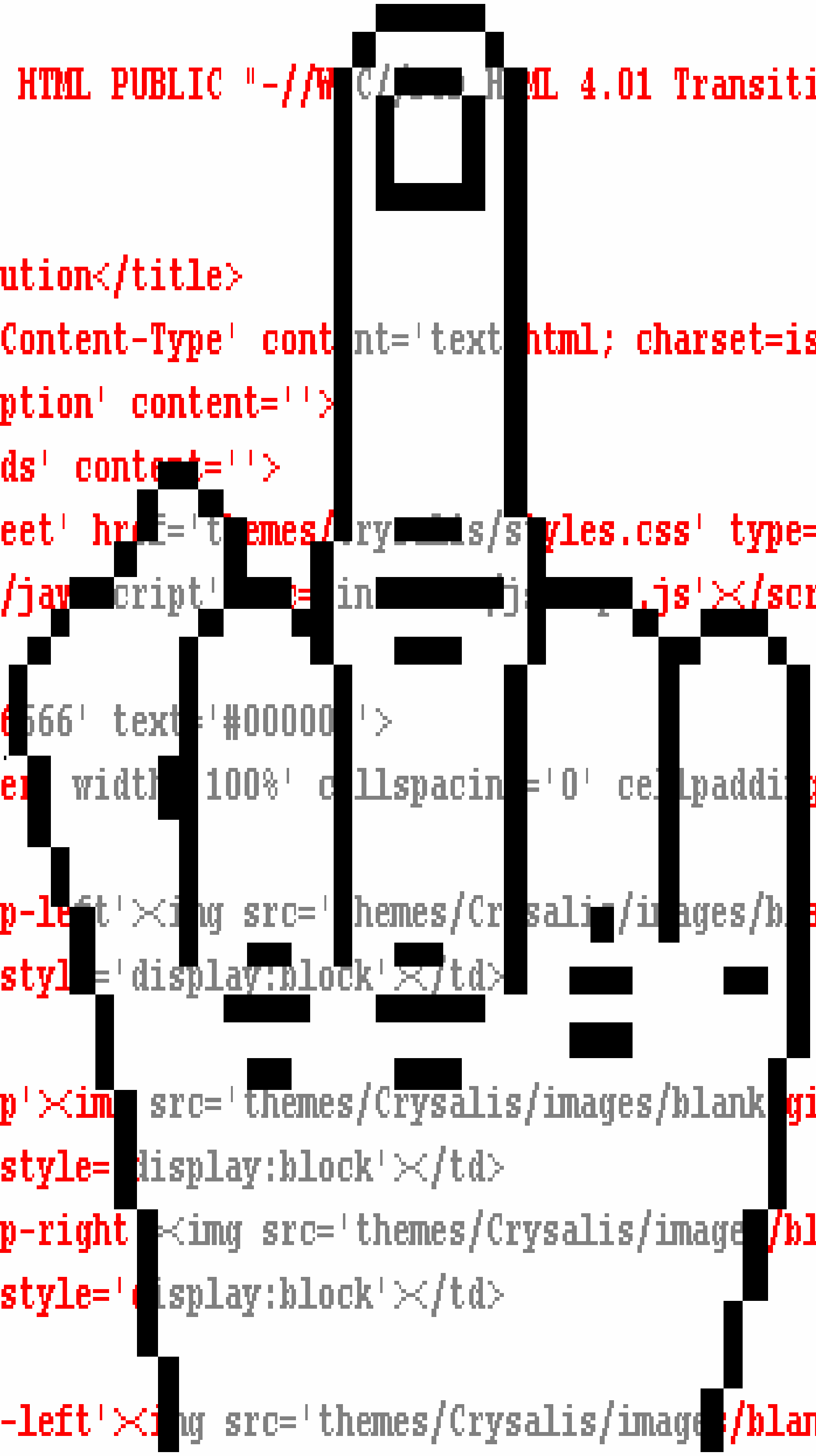
HACKING ETC.

ARSENAL KIT FOR DISOBEDIENCE

FALL 2005



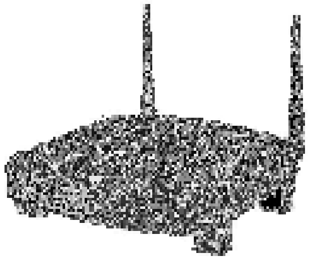
```
<SCRIPT LANGUAGE=javascript>
function show_hide(msg_id){
        msg_id.style.display=msg_id.style.display=='none' ? '' : 'none'
}
</SCRIPT><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Secure Evolution</title>
<meta http-equiv='Content-Type' content='text/html; charset=iso-8859-1'>
<meta name='description' content=''>
<meta name='keywords' content=''>
<link rel='stylesheet' href='themes/Crysalis/styles.css' type='text/css'>
<script type='text/javascript' src='includes/jscript.js'></script>
</head>
<body bgcolor='#666666' text='#000000'>
<table align='center' width='100%' cellspacing='0' cellpadding='0'>
<tr>
<td class='tbl2-top-left'><img src='themes/Crysalis/images/blank.gif' width='6'
height='6' alt='' style='display:block'></td>

<td class='tbl2-top'><img src='themes/Crysalis/images/blank.gif' width='1'
height='6' alt='' style='display:block'></td>
<td class='tbl2-top-right'><img src='themes/Crysalis/images/blank.gif' width='6'
height='6' alt='' style='display:block'></td>
</tr>
<tr><td class='tbl-left'><img src='themes/Crysalis/images/blank.gif' width='6'
height='1' alt='' style='display:block'></td>
<td class='header'>
<table width='100%' cellspacing='0' cellpadding='0'>
```

TABLE OF CONTENTS

A Breif Overview of FTP p.3
FTP is a protocol , a set of rules on how files should be transfered over TCP/IP. A standard FTP connection consists of a client and a server…

5 Ways to Improve Your Wireless Network p.4
While installing a wireless network may seem trendy, it makes good business sense. You have the flexibility and convenience of working un-tethered, plus you won't have to pay someone to come in and reroute network cables if you hire new employees or reconfigure your office floor plan. Setting up a wireless network requires thought and planning…



Changing The Name on Your Recycle Bin p.6
This nifty registry hack will let you change the name on your recycle bin to anything you want. Enjoy!

Simple Network Security p.6
The first thing we will discuss is passwords. Passwords are the first way a cracker will look to break into your system (via account brute forcing), so your passwords need to be strong…

Java Programming p.7
Java was created by James Gosling, Bill Joy, and many other people I believe at 1991 in Sun Microsoft. It was originally for box top TV-boxes. Fortunately, box tops were a failure, and they got the idea of Oak being an Internet language. Through development, someone got the idea of calling the language Java, and the name stayed. Java was released to public through beta stages, and eventually in 1995, Java became official at 1995(I think), at JDK 1.5, update 3.

Wal-Mart Wall Scanners p.10
While walking in Wal-Mart you might notice little devices meant to scan bar codes and report the price to you (the consumer) attached to poles through out the store. These things surprisingly are fun to play with and can do more then you would think at first glance.

ONLINE PDFs OF HACKING ETC.

You can easily get the free PDFs of all past issues of Hacking Etc. by visiting the site:

http://cholt.net/hackingetc

SUBMIT YOUR ARTICLES

We are always looking for people to submit articles for future issue of zines. You can get information on submitting articles by visiting the Hacking Etc. site currently located at the address above.

HACKING ETC. BETA SITE

We have been working hard on setting up a basic site to house all issues, contact information, and other information on submitting articles, passed issues, release dates, mini-zines, etc. Check it out at:

http://cholt.net/hackingetc

OTHER MEDIA

Teen Tech Talk
Teentechtalk.com

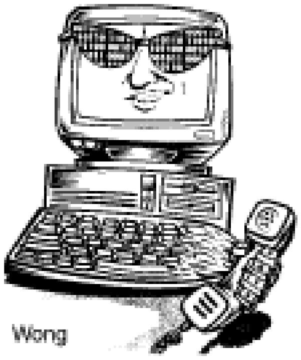
Teen Tech Talk is a weekly podcast produced and hosted by teens talking about the latest technology, technology flaws, etc. Visit the main site for more information.

GeekSpeak TV
Geekspeak.uni.cc

A tech based IPTV show focusing on the basics to advanced using and exploiting of computer systems.

How2Hack
How2hack.net

H2H is a website focusing on letting people learn all about computer security. Then we have challenges that let people use those skills in a controlled, legal environment. Check it out.



A BREIF OVERVIEW OF FTP (FILE TRANSFER PROTOCOL)
BY: OMNIPRESENCE from how2hack.net
ARTICLE FROM: hackerx.net

FTP is a protocol , a set of rules on how files should be I over TCP/IP. A standard FTP connection consists of a client and a server. The client opens a connection on the server which usually runs on port 21 and retrieves the file he wants. Once a connection is established , the server will send the client a greeting which usually looks like this:

220 Someone’s FTP server. Please login!

After the greeting , the client can send commands to the server , commands which are composed of verbs and sometimes parameters associated with them.
Here is a list of some common verbs:

CWD Change the current directory on the server.

PWD Print the current directory on the server.

CDUP Moves up to the parent directory.

LIST List the contents of a directory.

MKD Creates a directory on the server.

RMD Removes a directory from the server.

DELE Removes a file from the server.

USER Sends the username for the login.

PASS Sends the password for the login.

ABOR Abort the transfer.

QUIT Closes the connection with the server.

STAT Gets the current status of the server.

TYPE Toggles the binary flag on the server.

PORT Asks the server to connect to the client.

PASV Requests a data connection on a new port.

RETR Requests the server to send a file.

STOR Sends a file from the client to the server

APPE Same as STOR, except data is appended.

REST Start a download at a certain position.

SYST Gets the OS information of the server.

HELP Get help on a verb.

NOOP No operation.

One should only process one request at a time, waiting for the server to supply to that request although there are some verbs which can be given to the server at any time. These verbs are: ABOR, STAT and QUIT.

The server’s response are preceeded by was is called completion codes. We already saw one on the greeting banner. Generally the second digit being a 0 implies a syntax error ▯essage whereas a 2 implies a greeting message.

Now a complete connection looks like this (remember that every server response is preceeded by a 3 digit number):

```
220 Someone’s FTP server. Please login!

USER XIII

331 Username okay. Send password!

PASS password

230 Password accepted, usre logged in.

CWD ./files

250 CWD command successful

TYPE I

200 TYPE set to I

PASV

227 Entering passive mode
(206,84,161,87,28,46)

RETR datafile.zip

150 Opening BINARY mode data connection for
datafile.zip

226 Transfer complete
```

Now when you look at this you might be wondering what all these numbers after the passive mode are. The first 4 numbers make up your IP address and the 2 last ones specify the port to connect to. The port number is found by multiplying the first number by 256 and adding the second number. Here it would be (28*256+46)=7214. Now that the server has responded to the PASV request , there are now 2 channels: the communication channel for requests and the data channel for the data transmission.

One last thing to say about FTP is anonymous FTP. It is possible on some servers (companies or universities for example) to connect anonymously that is connecting with ‘anonymous’ as a username and your email address as a password.

CREDIT TO:

XIII
numberXIII@Phreaker.net

from: h4ckerx.net

5 Ways to Improve Your Wireless Network
BY: Omnipresence
From: Hackers Center

While installing a wireless network may seem trendy, it makes good business sense. You have the flexibility and convenience of working un-tethered, plus you won't have to pay someone to come in and reroute network cables if you hire new employees or reconfigure your office floor plan. Setting up a wireless network requires thought and planning. We spoke with Doug Potts, a security specialist at CDW, to find out what you can do to ensure their network works as smoothly and as securely as possible. The five steps to improving your wireless network are listed in order of their cost and complexity. Whether you take one or all five depends on the size of your budget and the level of security you need.

11. Set Up Wireless Encryption

Encrypting your network makes it difficult for hackers to crack in and use your wireless connection, access your data or other perform other malicious actions. "Encryption's an effective hacker deterrent," said Potts. "The thought of trying to hack a 128-bit or 256-bit cipher is enough to send a hacker packing â€" and looking for an easier target."

You have two types of encryption from which to choose: WEP and WPA with AES encryption. Potts likened 128-bit WEP encryption to a barking dog that frightens off a burglar. "Now AES, that's 256-bit â€" an even tougher type of encryption," Potts said. "That's like having the dog, an alarm system and a guard out front."

According to Potts, the 128-bit WEP encryption can be cracked, but it can take up to four hours of work to do it To date, he says, 256-bit AES has never been cracked.

Most wireless access points (Aps) support both WEP and WPA standards, but not all client cards (the Wi-Fi card that plugs into your laptop) support AES encryption, which requires a dedicated chip.

"At the very minimum," said Potts, "everyone running a wireless network should have WEP installed and turned on."

Typically you'll pay about $50 to $100 more for an AP that supports AES. Potts says that if you're installing a wireless network for the first time, it's a good idea to invest in the security features that WPA offers. If you already have a wireless network, Potts recommends upgrading all of your Aps to WPA over time as your budget allows.

2. Stick With the Same Vendor

Buying your Aps and Wi-Fi cards from the same vendor increases your network performance and reduces compatibility issues, since not all vendors support the same features. Potts sited a feature called "Turbo mode" as an example.

"Some manufacturers build a Turbo mode into their Aps and Wi-Fi cards," he said. "It's supposed to double your network throughput, but it only works if all your cards come from the same vendor. It could even be available only on a specific card within a vendor's line."

Potts continued, "D-Link has an AP and a Wi-Fi card that are specific to the Turbo mode feature. The company makes lots of cards and Aps, but not all of them support that feature. This is true of most vendors," Potts said.

3. Do a Site Survey

Potts likes to ask his customers a question â€" Do you know where your wireless signal is? Unless you know exactly how far your wireless network reaches, and in what directions it travels, chances are you're leaking a Wi-Fi signal that anyone with a laptop and a Wi-Fi card â€" including hackers â€" can use for free.

"A site survey will tell you exactly how far your signal reaches," said Potts. "Take your laptop and Wi-Fi card and call up the utility that measures signal strength, [each maker has it's own â€" Cisco's is called ACU] and walk around your office with the utility running. That will tell you how far the signal reaches and the signals strength," said Potts. There's also lots of software that can help you do site surveys, such as the programs from Wireless Valley.

"If the signal's strong throughout the office, then go outside and keep walking around to see how far it leaks," he said. "I work on the fifth floor of a building in downtown Chicago, and when I'm in my office and I turn on my laptop, I can access the unprotected network from the coffee shop on the first floor."

Small businesses need to be aware that their network's AP signal could be traveling further than they want and creating a potential security breach. Potts pointed out that encryption offers a good deal of protection, but the longer someone has access to your network, the greater the chance they can crack it.

"Remember WEP encryption can be cracked," [argh] said Potts. "If your signal leaks out into the parking lot, you're giving someone the time and opportunity to hack you. If the signal's contained to your office, you significantly reduce the likelihood of an outside attack."

4. Place Your Wireless Network on Its own VLAN

Potts explained that a VLAN, or Virtual Local Area Network, is a way of segmenting your network so that employees can access only the job-related resources they need without having access to the entire network.

"Not everyone needs to know everything," said Potts "This is a way to add a layer of internal data protection to your business." This is a somewhat more costly addition to a wireless network, but a good option if your business requires compliance with HIPAA or other types of state and federal regulations or you want to make sure that your personnel or other backend data isn't readily accessible.

Potts pointed out that high-end equipment manufacturers typically support VLAN capability. "You'll find VLAN in Cisco, Proxim and 3Com products," said Potts, "but not in Linksys, D-Link or NetGear."

5. Set Up a Secondary Authentication Mechanism

Authentication is a way that people can prove they are who they say they are in order to access a network or any secure area. The most common authentication method is the user name and password. Potts said that companies that deal with highly sensitive data might want to consider adding a second method on top of the type they currently employ.

"Of these five steps, this is the most expensive option," he said. "A company would need to invest in a RADIUS server, which can range anywhere from $3,000 to $8,000 dollars depending on the size of the company."

However, a number of low cost solutions for small businesses exist to help them use authentication servers that utilize the protocol called 802.1X. They include software packages like LucidLink or Elektron that runs on a local computer to turn it into a RADIUS authentication server, or hosted RADIUS like WSC Guard or WiTopia.net.

What kind of company would need this high level type of security? "This is mostly used in hospitals or medical practices that need to comply with HIPAA regulations," said Potts. "Other fields include financial services that must comply with Sarbanes-Oxley or industries with the money and the need to install a locked-down wireless network."

By Hackers Center

CHANGING THE NAME ON YOUR RECYCLE BIN

Written By: Omnipresence @ HOW2HACK.NET

Ok then, here we go. First off, you are going to need notepad and a small registry script that I provide for you. Now then, first open notepad and copy the following lines of code into the notepad:

```
[HKEY_CLASSES_ROOTCLSID{645FF040-5081-101B-
9F08-00AA002F
954E}ShellFolder] “Attributes”=hex:50,01,00,20
“CallForAttributes”=dword:00000000
```

Then hit save as. You want to save it as rename recycle bin.reg. This will make it a registry patch. When you open it, there will be a message box. Click yes when you see it. Then another message box will appear. Click OK. Now you are all finished! Go to your recycle bin and right click on it. Now there should be a rename button. Click it to rename the recycle bin just as you would any other file. Hope you learned something from this! Enjoy!

SIMPLE NETWORK SECURITY

WRITTEN BY: n3w7yp3 @ HOW2HACK.NET

The first thing we will discuss is passwords. Passwords are the first way a cracker will look to break into your system (via account brute-forcing), so your passwords need to be strong. They should contain uppercase [A-Z], and lowercase [a-z], in addition to numbers [0-9], and symbols [!@%^&*()-{}?<> etc). Also character length is important. The longer it is the harder it will be to crack. For instance, a 6 character alphanumeric password (a-z, 0-9), has a mean crack time of just over 10 hours. However, a password that is 10 characters and contains symbols (~!@#$%^&*()+=<>?:; etc), in addition to alphanumeric has a mean crack time of over 60 days. Makes a big difference huh? Admin passwords (especially for Windows) should contain ASCII non-printable characters. This will Stop L0pht crack from cracking the password. Also, never use a dictionary word (eg: test) as a password or a variation of a dictionary word (eg: test9). These will be cracked quite fast and if you use one well, you have screwed yourself.

Now, passwords can always be cracked eventually (keyword here is eventually), but there are new cracking methods that are being used to speed this up. The Password Probability Matrix is one such example (get some sample code for it at http://www.phiral.com). Basically it uses intersections and collisions in the hashes to eliminate possibilities and thus speed up a brute-force. Rainbow Crack uses precompiled hash tables and is similar to a PPM but not quite. The difference is that Rainbow Crack does not vector the give hash in a matrix (but it is still faster than using a standard brute-force). There is also quantum factoring and forcing elliptical curves on the cipher text, but the conditions needed for these attacks are so rare that you will not have to work about them anytime soon(in fact, at this stage they are mostly theoretical). If you are interested in checking the strength of your password hashes, I suggest you download john the ripper. It is available for free at http://www.openwall.com/john.

NOTE: The algorithm you use matters! For example MD5 is much more secure than DES. To see if you are using DES or MD5 as root cat out /etc/shadow (if it does not exist then your password hashes are stored in /etc/password and you’re screwed, it is publicly readable. Download the shadow suite ASAP!). if your passwords start with $1, then its MD5. if you see $, it is Blowfish. If all you see is a bunch of garbage, then chances are it is DES.

Of course, attackers don’t have to grab your password hashes to successfully crack your passwords. Then can do an online brute force attack (more accurately called an automated dictionary attack). Basically how this works is you take a list of words, feed them into a program, and specify a target host/port. The program then tries a username that you specify (or it guesses a few), and proceeds to try and login using the words in the dictionary file. If you are interested in trying this attack on your system, I suggest you use THC-Hydra. It can be downloaded for free from http://thc.org/releases.php. The next thing you need is a dictionary file. I have one that I would be more than happy to send you. It is 11MB (that’s 1,119,380 words) with no repeats.

Trust relationships are our next topic. A trust relationship is when one computer trusts another. An example of this is the (in)famous *nix .rhosts file. This will allow people to login and execute commands on the system with *no* username/password. In fact if the contents of the .rhosts file are simply “++”, (no quotes), then *anyone* has instant access. If this file is placed in / or /root then *anyone* has instant root access. And don’t think that if you risible the “r” services (rshd, rlogind, rcpd, etc) you’re safe. If you use this file with SSH, you’re still vulnerable. To sum it all up, don’t let any computers you own have a trust relationship with *any* other computer!

Basic network structure comes into account as well. Say you have a server. Now, which is more secure, setting up a DMZ or using port forwarding? If it is in a DMZ, then it is completely open to attack and is no longer protected by the router. If you opt for the DMZ, be sure to use iptables or some other firewall to lock the host down hard and regularly scan it and run AV (rkhunter and chkrootkit for Linux, Norton or some other AV for Windows). Also, disable UpnP and VPN tunneling at the router if you don’t need it. Your router should also block ICMP and expired UDP packets. This will protect you from ping and traceroute (and tracert).

On the LAN things are a little different. The router will stop 95% of attacks into your LAN. At this point, the only realistic way in is through client side attacks. Of course, if you use a server with port forwarding, then the protection is less, as people can talk to the server which is inside of your LAN. All your hosts should have good paranoid firewall rules (block all inbound TCP and UDP), and should monitor outbound connections (important for Windows, not so much for *nix as Windows has more outbound exploits). *nix hosts (especially Linux), should have the various RPC services turned off, along with unneeded daemons and services, and Windows hosts should have NetBIOS and SMB file sharing disabled (of course be sure to block NULL sessions). On top of that, again all hosts should deny all inbound TCP and UDP. You can never be to paranoid... ;) .

Once a week, be sure to give your box a scan with nmap (http://www.insecure.org). nmap is perhaps the best port scanner ever. Also, be sure to run chrkootkit, available at http://www.chkrootkit.org, along with rkhunter (get it at http://www.rootkit.nl/projects/rootkit_hunter.html). If you have Windows hosts, be sure to run AV on them too. And keep your scanners updated! An old AV scanner is as bad as not having one! Also, be sure to keep up with the patches!

Just think about how a network is normally hacked and go from there. Try and hack into your own network. You may find that it is secure. Or you may find that it has some gaping holes.

JAVA TUTORIAL 1 JDK 1.5

WRITTEN BY: CHEESE @ HOW2HACK.NET

History of JAVA

Java was created by James Gosling, Bill Joy, and many other people I believe at 1991 in Sun Microsoft. It was originally for box top TV-boxes. Fortunately, box tops were a failure, and they got the idea of Oak being an Internet language. Through development, someone got the idea of calling the language Java, and the name stayed. Java was released to public through beta stages, and eventually in 1995, Java became official at 1995(I think), at JDK 1.5, update 3.

Sun Microsoft allowed Java to license in which that anyone can make an implementation of Java. There are people at work, making an implementation of Java, hoping Sun will give a certification stamp to their product.

FYE

Something to clarify:

Sun Microsoft is not Microsoft (You don't know how many people think it is).

Sun Microsoft is not a software company. They make servers.

What is JAVA?

Java is an object oriented programming language. It is a powerful Internet language, and has three versions, J2SE, J2EE, and J2ME. J2SE is Java 2 Standard Edition, J2EE is Java 2 Enterprise Edition, and J2ME is Java 2 Micro Edition. J2SE is for desktops and laptops, for your typical computer application. J2EE is for businesses, which cover customers by the millions (such as services, ect.). J2ME is for cell phones, cameras, anything with a JVM (which we will cover later). There is also Java Card, used for little cards used for identification, ect.

Not only is Java a useful Internet language, yet it is also cross platform (in other words, compatible with multiple OS).

Some stuff to note:

Java is not slow (That used to be true many years ago). JDK(Java Development Kit) 1.4 took care of this issue.

Java has about equal power as your typical language.

All languages trade off certain abilities to gain other abilities. For example, Quick basic trades off functionality for simplicity. C++ trades security for speed. Of course, almost all languages trade off cross platform, for usually executable code. Also note that Java is an application language.

Note: Java isn't a recommended hacking language. It wasn't made in mind for hacking.

Should I Learn Java?

You should learn if:

You want to write application programs available for all OS.
You want to write a game (By the way, Java supports FSEM (Full Screen Exclusive Mode) and 3-dimensional graphics (J3D).
You want to get a programming job. Believe it or not, Java programmers are in the highest in demand. (If you want a job in Java, I recommend learning J2SE and J2EE)
You want to write an internet application (a message client like AIM or a MMORPG)
You like free stuff. (There are many people like that. My friend is obsessed with free food)

You probably doesn't want to learn Java if:

You are 100% dedicated to some language and self chose not to learn Java.
You are a Microsoft Windows fan, and support their (illegal) monopoly (I think it was illegal)
You are obsessed with really powerful hacking languages.
You think C# is better that Java. C# is a programming language made by Microsoft. It is just like Java and J++ (Another clone by Microsoft), except that it only works on Windows.
You are too lazy to learn a new language.
(If 2 or more of these options apply to you, you should consider not reading this tutorial)

Beginners may not attempt to learn Java at first. Try for a more simpler language, until you get better. I would recommend:

Quick Basic
HTML
Basic
Afterward, consider migrating to Java

A Few More Things

This tutorial is few of a series (depending on feedback). Got any comments, suggestions, or questions? Ask at the discussion forum (Don't be mean.).

This tutorial will cover mostly basics.

Installing Java

This isn't too difficult.

11. **Go log on to java.sun.com**

This site is based on Java (It recently had a site make over). Get all the news on Java.
While waiting for JDK 1.6. Of course, there are other things to check out.

2. Take a look at the main page
See the menu at upper right that says Popular Downloads Find JDK 1.5, or what ever is available. DO NOT DOWNLOAD ANYTHING ELSE BESIDE THE JDK!!! YOU WILL REGRET IT LIKE I DID!!!

3. Click on it.
This is where everything divides!

You can download JDK with NetBeans or without. With NetBeans, you are adding the burden of an extra 40-50 MB (The JDK alone is around 50 MB).

NetBeans is an IDE. For people who never heard of it, it is Integrated Development Environment. It is for people (like me) who cant set up a class path, or have difficulty compiling a program within a command prompt. I used NetBeans, and I would only recommend it to people with Linux computers. (I can never set up a class path on my Linux computer).

Overall, the benefit of IDEs are that you save trouble setting a classpath. However, you may be sick of the program layout. Its your decision.

4. Read the license agreement, and agree.
If you don't, you cancel download the JDK. The agreement is about copyrights and software agreements of JDK.

5. Download the JDK version for you OS.

6. Wait. 50 MB download is long (for me)
Afterward, you are ready to install.

7. Run the installer.
It takes a while to load up. Afterward, you will then enter the installation screen.

8. Agree to agreement.

9. Choose what to install.
The installation is huge at over 200 MB (without NetBeans). If you need every bit of space in your hard drive, consider slimming the installation.

10. Wait for everything to install.
2 installations will take place. One is for JDK 1.5, and one is for JRE (Java Runtime Environment). Glad you just downloaded only JDK (hopefully)?

11. Exit when done.

Superb! We installed Java! Now, there are now 2 paths to follow- working on command prompt or an IDE.

Working with Command Prompt

You will need to set up a class path to do everything.

Set path variable on your OS.

Ex. C:\Program Files\Java\j2sdk1.5.0\bin

In XP, go to following:

Start->Control Panel->performance and maintenance->system (should be in that order)
Then, click the advanced tab, environment variables at the bottom. Choose a path on System Variables.

Add your path (ex. C:\Program Files\Java\j2sdk1.5.0\bin)
Must have /bin as final part.

If this seems not to work, go onto http://java.sun.com/docs/books/tutorial/getStarted/cupojava/win32.html

Working With IDE

Get an IDE, any IDE. If you use Windows (Like me), get Jcreator (www.jcreator.com), or if you use Linux (Also like me), get NetBeans.

Just directly install, and the IDE will usually take care of the rest.

We are now done with Java installation

Example Code

You can find example code at http://how2hack.net.

Conclusion

Learn the very basic.

You have just seen a little of Java. Very little. I plan to cover more in tutorial 2.

There! That was a lot to read. Unfortunately, to save some space, I'll stop here. Sorry if I made you bored The next one should be smaller.

Next tutorial will probably cover:

Variables: String and numeric
Arrays
Methods

Hacking Wal-Mart Wall Scanners
By: LexDysic From: DocDroppers.org

Overview:

While walking in Wal-Mart you might notice little devices meant to scan bar codes and report the price to you (the consumer) attached to poles through out the store. These things surprisingly are fun to play with and can do more then you would think at first glance.

First, Lets go over the basics of the device:

- Take item with a UPC bar code and scan it on the underside.
- Wait a second and watch as the price of the item appears on the screen.

Seems simple enough, eh?

Now lets go over some features that you probably didn't notice at first:

- Touch screen
- 802.11b/g equipped
- Setup mode
- MSR(Magnetic Strip Reader)
- (maybe more to be discovered?)

Staying Safe:

Now remember, these price scanners on the walls are for YOU to play with. So if you get caught by a "Wal-Mart Associate" or a "caring shopper" simply reset the box (explained below) and shout something like "DAMNIT I died at level '42' AGAIN!" Then simply walk off and find another box or come back in like 2 mins.

NOTE: Wal-Mart Associates do not care what you do. However "caring shoppers" will rest at nothing to make your day hard. Remember, Wal-Mart Associates can be fired if they try to kill you, but shoppers won't get fired. So be careful. A lot of whack-jobs shop at Wal-Mart. I have had some close calls with NASCAR fans who got mad at me for helping them pick up some stuff they dropped. Another time, me and a friend got chased around by some lady with three kids who saw us use the "Courtesy Phones." Anyways, long story short if someone freaks out because you are doing something they don't (can't) understand, just WALKAWAY.

That ends my rant on avoiding crazy people...

Setup Mode:

Setup mode contains a wealth of information and options. But first, we must enter setup mode. This can be simply accomplished by approaching the device and looking on the pole for an 110v power outlet. The scanner should be plugged into this outlet. From there simply unplug the AC adapter then plug it back in to force the scanner to reboot. While it is rebooting it will Prompt you to tap the screen to enter "Setup." Do as it says (because it's a good Idea to do what Wal-Mart says to do.) From there it should ask you to tap the screen on the crosshairs to calibrate the touch screen.

Now pat yourself on the back! You have successfully completed the first half of the entering setup mode.

Ok, back to work... You should be sitting at a password prompt with a touch screen keyboard bellow. Now when I first saw this, I tried to top 4 passwords from the movie "Hackers." Sadly, this flopped (just like the screenplay should have). Then after a quick manual brute force, the password turned out to be:

<u>Calibrate</u>
Lets you calibrate the touch screen for your finger/pen.

Brightness

Allows you to change the brightness of the LCD screen.

Host

Lets you select what port to use when connecting to host. Ports available are 64-69. Default is 68.

Rest

Resets the box... Duh!

System Info

Displays all sorts of info including hardware and software versions. System Info also reviles that this system is running DOS. Although it does not say it, it uses files with extensions such as: .bat, .exe, .bin, etc...

Test

This option is really cool in my opinion. It allows you to play with all the little extras on the price scanner! Here is what you can do:

Audio

Performs a sweep. Its kind of fun to tap this then watch as people look around to see where the annoying noise is coming from.

Touch Pad

Simply tests the touch pad.

COM

Lets you test the COM1 port. I could not figure out what was attached to it so I am guessing it was empty.

Smart Card

Tests the smart card... If you have one.

Network

Displays your MAC address, Local IP address, and gateway.

MSR(Magnetic Strip Reader)

This is one is really cool. It lets you test the MSR and find out a little info on wal-mart ;) Anyways, the MSR will read 3 tracks of data. I left my wallet at home so I tested it on wal-mart phone cards. The MSR also tries to pick out these field: Issue, Account No., Name, Expires, Service, Name, City, State, Address, First Name, Middle Name, and last but not least... Last Name. (can anyone guess what kind of car it is looking for?)

Download

I could not access this option because it was grayed out. It would appear that it would let you download updates to the client software it was running.

Time and Date

I shouldn't have to tell you...

Network

This is another fun tab. Here are some of the options... I really think that they should explain themselves:

- SSID
- Broadcast Add.
- Gateway
- Primary DSN
- Secondary DSN
- WEP Key(yes, it lets you view this in plain text with no authentication)
- Device Name
- Device CID

- Static IP
- Subnet Mask

There you have it, you can easily map your local Wal-Marts network.

Exploration:

There are more things you can do here. I figured that if you are reading this you should be smart enough to figure out what else you can do. Remember, retail hacking is all about exploring and figuring stuff out for yourself.

Here are some more ideas for things you can try:

- Getting a Command prompt.
- Setting up an Ad-Hoc network with the price checker.
- Changing the greeting.
- And whatever your twisted mind can think up.

There is a lot you can do with these devices Explore, have fun, and if you send me some feedback I will be more than grateful. At this time I want to learn as much as I can about these things because so far it has been a blast playing around with them. And its funny how something so simple has so much power.

Thanks for reading this, I hope someone finds use or amusement for this...

SHOUTS for Comutron... and for everyone who ever worked on PWF at http://www.oldskoolphreak.com

NOTE: Nothing in this file ever happened. I made it all up. I am a liar. Do not try this, at home. This is just a story I heard from a little bird named Billy who was shot in a strange hunting mishap!?