Aelphaeis Mangarae

Denial Of Service FAQ(Basic):

Contents

INTRODUCTION:

This information text is for network administrators who know little about Denial of Service, this text covers all the basic information on Denial of Service attacks and related information.
Denial of Service attacks are becoming more and more common on the internet, it does not take a sophisticated hacker to set up and launch a denial of service attack, rather the most common attacker is a young script kiddie, they can accomplish a lot just by using tools downloadable on the internet.
Denial of Service attacks are becoming a huge problem on the internet recently because of how easy they are to perform, many online banks and casinos have been attacked because they refused to pay a sum of money to the attacker(s), law enforcement have seen people with more than a gigabyte per second of bandwidth and at the moment the problem seems to be increasing, right now there Is probably someone out there with more than a Terabyte a second of bandwidth, a gigabyte per second is enough to take down servers such as yahoo.com and amazon.com
You cannot prevent Denial of Service attacks, but its useful to know abit about it so if your server is attacked you can possibly stop the attacks or prevent them from being severe.
This tutorial was written by Aelphaeis Mangarae!
BY READING THIS ARTICLE YOUR AGREEING YOU HAVE READ THE DISCLAIMER AND AGREE TO IT.

Aelphaeis Mangarae

DIFFERENT METHODS OF DoS:

DoS:

A DoS attack is when the attacker launches an attack from his or her own computer, this is done by sending packets of data to the remote computer, for each packet sent the target machine receives one, this is a very uncommon form of denial of service because the attack most of the time is very unsuccessful and at times can be easily traced.
DoS attacks are usually carried out by amateur script kiddies who have no idea what the “hacking tool” there using actually does at all, they think they have a chance of taking down a web server just using there own computer, most of the time the script kiddie finds out there wrong and moves on to use another “hacking tool” or possibly uses tools to perform DDoS (Distributed Denial Of Service) attack(s)

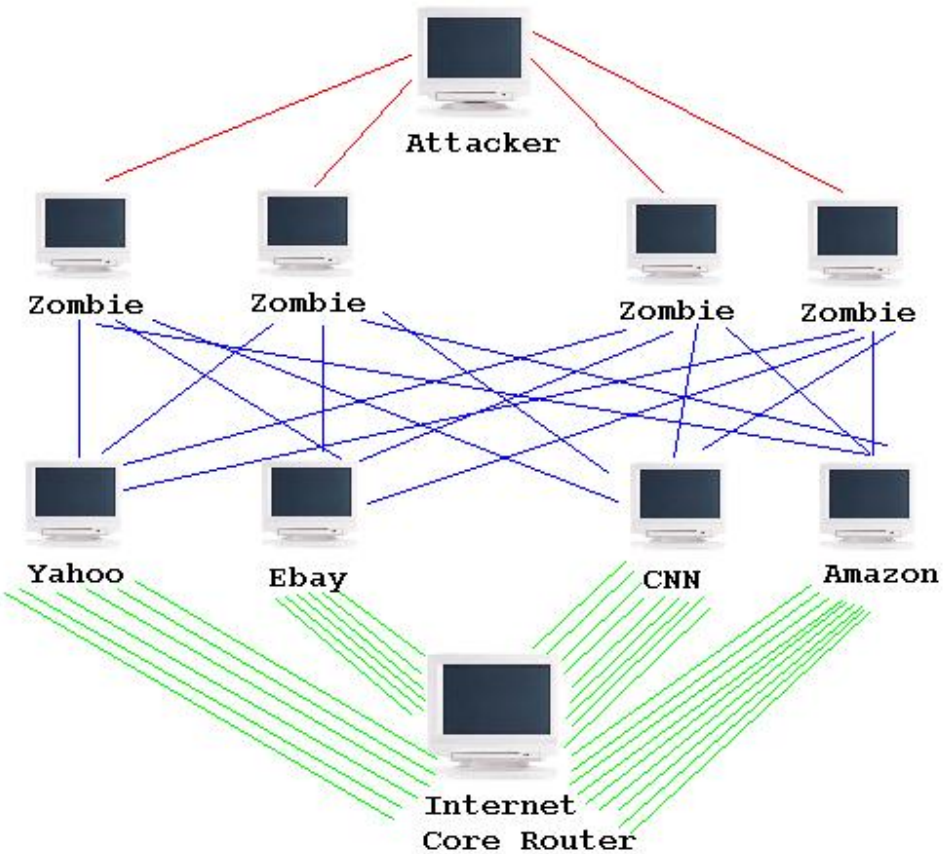
DDoS:

DDoS (Distributed Denial of Service) attacks are the most common form of denial of service an attacker uses.
If an attacker wishes to launch a Denial of Service attack, he infects thousands or even tens or hundreds of thousands of machines with a bot, usually this bot logs into an IRC chat room from the infected machine and waits for the attacker to give commands, the attacker then types in a command for example “$flood ICMP www.yahoo.com” the bots in the IRC room receive this command and send ICMP packets to the remote target, because the attacker has so many bots and the bots are on fast servers the attack is often successful in shutting down the remote target or denying service to legitimate users trying to access that server.
Sometimes the attacker chooses to manually infect victims that he or she can use for attacks, the attacker usually does this by making an IRC bot that goes into IRC rooms and uses social engineering to get people to visit a website that exploits a security hole in Internet Explorer (generally Internet Explorer because its so insecure) and downloads his bot onto there computer.
Recently building up a large “army” of bots to use for attack has become quite easy, there are many bots on the Internet available for download such as Forbot, RxBot and Agobot, these bots spread by scanning the internet for certain ports/services and attempting to exploit them and infect the remote computer, this type of spreading can be very useful when the bot is using a **0day exploit.**
DoS bots usually have standard flooding, such as **ICMP**, **UDP**, **TCP**, and **SYN** Flooding.

Aelphaeis Mangarae

DRDoS:

DRDoS (Distributed Reflected Denial of Service) is quite an uncommon type of denial of service attack because usually it is not required to take down a large server, although was used once by the infamous “Mafia Boy” who took down cnn.com, yahoo.com, amazon.com and ebay.com
DRDoS is when an attacker sets his bots to flood different Inter-mediate hosts with spoofed packets, for example the attacker sets half his bots to flood yahoo.com with spoofed ICMP packets and half ebay.com with spoofed ICMP packets, the spoof packets look like they have come from microsoft.com so yahoo.com and ebay.com unknowingly flood microsoft.com, because the source of these packets is spoofed, ebay.com and yahoo.com will reply to the spoofed source, for each packet the attacker sends to yahoo.com or ebay.com its possible that yahoo.com or ebay.com may have thousands of machines on the same IP Address, each of these machines will reply to the spoofed ICMP packet, therefore amplifying the power of the attack greatly.
Below I have inserted a diagram showing how DRDoS works.



Red Lines: Connection from attackers from computer to zombies computer, that the attacker uses to tell the zombies to attack.

Blue Lines: Zombies sending spoofed ICMP packets, these ICMP packets look like they came from the Internet Core router the attacker wishes to attack.
Green Lines: Each of the computers connected to ebay.com, yahoo.com, cnn.com and Amazon.com are replying to the spoofed ICMP packets, therefore, flooding the Internet core router.

Note: I doubt very much someone would be able to use cnn.com or any other website like it as a inter-mediate host, however there are big networks out there that could used for reflecting packets off.

DIFFERENT TYPES OF DoS ATTACKS:

ICMP:

ICMP flooding is probably the most common type of Denial of Service attack, since nearly all websites reply to ICMP packets, its easy to use ICMP flooding to shut them down.
ICMP flooding works by sending a lot of ICMP packets to the target machine, for each packet sent the remote computer has to reply to each one, meaning it would exhaust the machines bandwidth so a legitimate user could not access the server.
ICMP packets are better known as “Pings”, they are used to see if a remote computer is online.

UDP:

UDP flooding is when the attacker sends garbage packets from UDP port(s) to UDP port(s) on the remote computer, since UDP is a connectionless protocol UDP flooding can be very effective.

TCP:

TCP flooding can simply be done by making thousands of connections to the remote computer therefore maxing out the maximum amount of connections the remote computer can receive, another form of TCP

Aelphaeis Mangarae

Flooding is when the attacker connects via TCP and sends garbage data, lagging the remote computer.

TCP SYN:

When a computer wishes to make a connection to a remote computer, it does what is called a **3 Way Handshake,** first the computer that wants to connect sends what is called a **SYN** packet, the remote computer then receives that packet and sends a **ACK** packet back, to confirm it received the **SYN** packet, the connecting computer then attempts the connection.
Obviously if you flood a remote computer with **SYN** packets, its going to send back an **ACK** packet wasting its bandwidth, not only that but if the remote computer never attempts the connection the target computer can be left waiting for a connection, therefore its possible to max out the remote computers connection ques, the amount of bandwidth this attack uses is very minimal, although if done on a very large scale could effect the bandwidth of a web server.

MAIL BOMBING:

This type of denial of service attack is usually done by amateur script kiddies, **Mail Bombing** is when the attacker sends thousands of emails to an email address flooding it, these attacks are usually pretty harmless.
However if coordinated correctly could be used to max out an SMTP server or possibly harass users of a certain ISP.
The extent to what this type of flooding could do, I think is greatly under estimated because this type of attack is only carried about my amateur script kiddies and has never been used on a large scale (yes i know you think its ridiculous.)
This type of attack doesn't really exploit bandwidth, although it could, but rather Hard Drive space and peoples time, having to delete thousands of emails can be a timely procedure, some free web based email services only let you delete the emails one by one, so obviously deleting the emails won't even be an option.
This type of attack most of the time is easily traced, all you need to do is get the source IP Address of the email, find out information on the ISP the attacker is using (do a Whois) and email them.

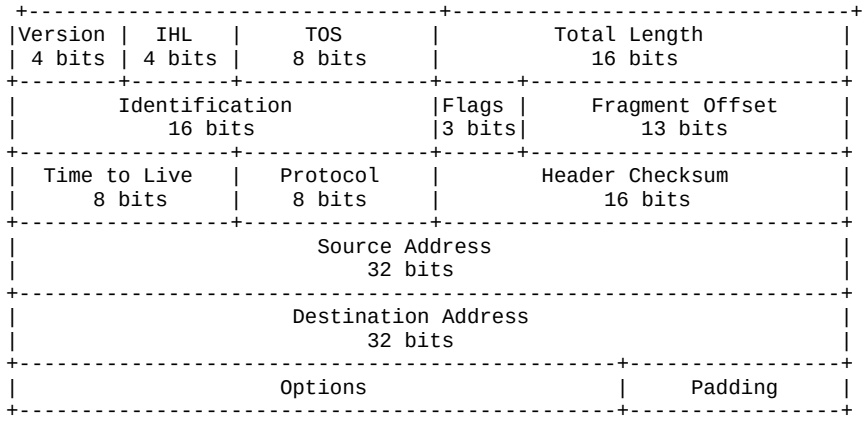
OTHER:

There are many other types of Denial of Service attacks, all DoS attacks are is when an attacker uses bandwidth to max out the bandwidth or other resources of another system or systems, a way an attacker could max out the bandwidth of a server could be by making his zombie computers load the webpage on a web server repeatedly, so all the bandwidth from the host computer would be maxed out.
Not that long ago Blackcode.com was attacked by a Denial of Service attack, the attacker used zombie machines to continually load the php modules of the forum on blackcode.com, therefore maxing out the server.

A good way of trying to prevent some types of Denial of Service attacks is by not allowing the same IP Address to make more than one connection to your web server therefore the zombie machines couldn't take up much bandwidth unless there were a lot of them making and connections and flooding.

SPOOFED PACKETS AND RAW SOCKETS:

Raw sockets are pretty much the same as normal sockets, except you are able to control the packets you send better.
With normal sockets you can supply information like the destination IP Address and the data to be sent with it.
You see with raw sockets, you are able to completely create the packet, including the **source address of the packet and TTL (Time to Live)** which of course could be faked.
All versions of Linux support raw sockets, however its only in Windows 2000, XP and 2003 (Winsock Version 2) that support raw sockets, however who still uses Windows 9x?
So if you have a good version of Windows it will support raw sockets, however many of you have heard of Steve Gibson.
I won’t go into to much details about Steve Gibson and his propaganda, but anyway, Steve basically said that script kiddies are going to use Windows XP to launch DoS service attacks and because it has raw sockets they could use ip spoofing “hack tools” which of course if you read this article is basically incorrect the attacks just aren’t effective and script kiddies aren't going to co-ordinate them effectively like Steve makes out, Raw sockets have been disabled in Service Pack 2, just as Steve Gibson wanted.
You don’t have to worry any more about attackers using DDoS bots that have spoofed packet support in them because SP2 does not support raw sockets so they can’t spoof the IP (at the current moment I don’t think they have found away to disable SP2’s raw sockets.)
However script kiddies know that SP2 disables raw sockets, so obviously there not going to download it.
Raw sockets will still be used in DDoS bots I’m sure that bot coders will soon find away around SP2 disabling raw sockets, if they haven't already done so, if someone attacks you and the IP Address of the packets is spoofed, it’s virtually impossible to trace them (using the packets that are sent at you.)
With raw sockets you can create the packet entirely, below is a diagram, of an IP header.



I stole the diagram from **Black Sun Research Facility**, so credits to them for the diagram.

PREVENTING DoS ATTACKS:

PROTECTING YOUR BOX FROM BECOMING A ZOMBIE:

Most DoS attacks are possible because an attacker has a large army of zombies to use to attack web servers, you can help stop this by making sure your computer is not infected with any type of bot.
There are several signs that may indicate that your computer is infected with one of these bots, such as:

1. Your computer shows a connection to a server on port 6667 (the port used by IRC) even though your not using an IRC Client and are not connected to IRC in any known way.
You can see the connections going to and from your computer by going into command prompt and typing netstat -n (will show IP Addresses and Ports.)

2. Your Anti-Virus shows that you are infected with a virus, however keeps terminating for an unknown reason, this is more likely to be caused by a trojan, however if your computer shows that you are infected with a bot, then this may be why your Anti-Virus program is terminating.

3. At certain times your upload bandwidth is very slow for an unknown reason.

4. Your firewall asks you if your wish to allow an unknown exe file to access to the internet so it can send ICMP packets to certain domain name.

5. Your firewall reports that windows explorer or another important windows program has been high jacked or changed since last time it has run and wishes to make a connection to a certain domain or send ICMP packets to a certain domain.

6. Your computer is not up to date with the latest security patches and the software your using is out dated, if this is the case its more than likely your computer has been compromised by a bot and infected, bots spread by using exploiting vulnerabilities, although some use 0day exploits, so updating your software and patching doesn't always help, so you might want to install a Firewall if you haven't already.
With bots constantly scanning the internet, if your computer is not secure its likely your computer is helping contribute to a DoS attack(s) on web servers.

7. For an unknown reason there is literally thousands of outgoing connections from your computer, this may be a bot connecting to a remote web server trying to max out the connection ques.

PREVENTING YOUR NETWORK FROM BEING A REFLECTIVE HOST:

DRDoS (Distributed Reflected Denial of Service) attacks can be very powerful, sometimes an attacker could go from having 100 MB of bandwidth, to literally tens of gigabytes using intermediate host(s) to reflect packets off, its very important that if you are a network administrator you are able to make sure your network cannot be used in a reflected attack against another server.
A good way of making sure your network will not reflect packets onto another network is to make sure that your network will only forward IP packets to computers inside your own network, you can do this by configuring your router to only forward packets to nominated IP Addresses, such as the IP Address of your website if you are hosting one on your network as well as network IP Addresses such as:

```
0.0.0.0/8          - Historical Broadcast
10.0.0.0/8         - RFC 1918 Private Network
127.0.0.0/8        - Loop back
169.254.0.0/16     - Link Local Networks
172.16.0.0/12      - RFC 1918 Private Network
192.0.2.0/24       - TEST-NET
192.168.0.0/16     - RFC 1918 Private Network
```

```
224.0.0.0/4         - Class D Multicast
240.0.0.0/5         - Class E Reserved
248.0.0.0/5         - Unallocated
255.255.255.255/32 - Broadcast
```

If you are using NAT (Network Address Translation) make sure you set filtering up properly between your NAT device and your ISP.
If you have your network setup its a bad idea to have Directed Broadcast enabled, having Directed Broadcast enabled is basically asking for someone to perform a reflective attack using your network, disabling Directed Broadcasting should stop all the machines connected to your network from replying to the same packet, hence prevent amplification of a DDoS attack.
After securing your network against reflective attacks its a good idea to test out your network, the following websites can test it for you:

http://www.netscan.org
http://www.powertech.no/smurf/

Beware though, if your website does reply to reflective packets and can be easily used in a reflective attack it will be added to a black list of networks which attackers can use for amplification so make sure you secure your network if for some reason your network can be used in a reflective attack.
Also its always a good idea to have a Firewall or IDS on each of the machines on your network, not only will it make your network less prone to reflective attacks, it should also help secure your network against hackers.
By default the following systems have Directed Broadcast disabled meaning they cannot be used to reflect packets off:

Cabletron SSR
FreeBSD
Microsoft Windows Workstation & Server 3.5 & 3.5.1

However in the following systems Directed Broadcast is enabled by default.

Windows NT 4
Cisco
Bay

Its very important if you are an administrator of a large network of even a small network that you disable Directed Broadcast so that packets cannot be reflected off your network, unless Directed Broadcast is needed, at which time you filter where the packets on your network are allowed to go carefully.

Aelphaeis Mangarae

YOUR SERVER IS BEING ATTACKED, WHAT NOW?:

Denial of Service attacks are very hard to prevent, especially if your not sure what your attacker is going to use against your server, but what if your server is being attacked, right now!
Well there are some things you can do, to temporarily prevent the attacker from slowing or shutting down your server.

If the attacker is flooding your server(s) with ICMP packets an obvious fix to this would be to make sure your server does not reply to ICMP packets, which it shouldn't if you have a firewall installed which of course you should of in the first place.
Microsoft recently made it so there website (microsoft.com) no longer replies to ICMP packets.

If your attacker is maxing out your connection ques, you could easily fix this by setting the amount of connections per IP Address to 1 connection, or blocking the connections from the IP Addresses that the infected machines are using (machines infected with bots.)

The attacker may be maxing our your website server by setting his or her bots to download a certain object multiple times, again this can be stopped by banning the IP Addresses of the bots.
You could possible delete the object which is being downloaded or move it to a different place on your server, this would stop the attacker temporarily, of course its likely the attacker may find the location of the object again and set his bots to download or access this object continually, but moving the object(s) multiple times may deter the attacker.

Another way the attacker may max out your service is by accessing a service on the service many times, this service may be one that isn't used that often, if you find the attacker is accessing a service which you rarely use, disable the service (at least while the DoS attack is going on.)
It's very important to have as little services as possible running, and during a DoS attack it might be wise to switch of services such as FTP.

The last method of all an attacker users to slow down or freeze a server is exploiting a Denial of Service vulnerability in a piece of software your web server is running.
It's very important (as i have probably mentioned many times) to keep your software up to date, Denial of Service vulnerabilities are found in software all the time, even web server software like Apache, you might want to subscribe to a security mailing list like Bugtraq, so you can keep up to date with all the latest vulnerabilities that are found.

CATCHING THE DDOSERS:

Many people let DDoS attacks happen and afterwards they do nothing about investigating the attack, if you are attacked it is possible to track down and apprehend the ones responsible for the attack, most of the time, the people that are launching Denial of Service attacks are just script kiddies and know little about what the tools there using

actually do, so it's easy to track some of them, below are some steps you can take to take down attackers.

1. Have a look at where the DoS attack is coming from, you will probably notice it could be coming from thousands of IP Address, most of the IP Address won't change because the infected machine is on an ADSL connection, now assuming the attacks bots cannot spoof/fake the packet headers the IP Address your seeing should be correct, do a Whois on several of the IP Addresses, get into contact with the ISP's that are providing service to the infected machines and email them asking them for the email address of the owner of the infected machine, or possibly ask for the ISP to tell the owner to contact you.
Once you have talked to owner of the infected machine, help him find the bot that is installed on his or her computer, this may be as simple as asking them to install an anti-virus program, get the owner of the infected machine to send you the bot.

2. You now have the bot, a bot which was used to launch attacks on your web server, it's not time to track the owner of the bot.
You will need the following things to have a chance of tracking the bot master.

Packet Sniffer (I recommend Ethereal http://ethereal.com)
The Bot
Computer to infect bot with
Netstat or program for viewing IP & DNS traffic (Optional)
IRC Client

Ok now infect a machine with the bot you have got, it's best to disconnect the computer from the internet first, now start up Ethereal packet sniffer, start sniffing for packets leaving your computer.
If you do not know how to set up Ethereal, here is a tutorial http://example.com/etherealtutorial.html
Now connect your computer to the internet, your packet sniffer should now show programs accessing the internet and the packets they are sending, i recommend that you have no other programs accessing the internet except for the bot.
Now you should notice the bot connect to an IRC server and send a password, well you should see the in the packet sniffer the server is connecting to and what its sending, so just look for some sort of URL probably a URL like no-ip or something sort of static DNS software, you should now have the IRC server and the password for it, which of course can be very useful, it's possible when packet sniffer you may of got garbage data, some bots show data that is not correct to confuse someone trying to track down the bot master, however the correct server of the bot should be there somewhere, a friend of mine who was trying to track down a bot network said the packet sniffer was showing the bot downloading an .swf, this was most probably the bot trying to confuse my friend.
I also must note sometimes bots download .txt files that contain information about the IRC server is must connect to, if this is the case your very luck, because all you need to do is find that txt file and download it from the web server hosting it, and bingo you have the IRC server information, sometimes the bots appear to download other file types such as .jpg however these files may contain the IRC server information just like a txt, it may be possible to open these files up in Notepad and find some interesting information inside.

It's also possible you may not need a packet sniffer for this, you could simply wait for the bot to connect to the IRC server and use a program like Netstat (comes with Windows) to check your TCP/UDP connections and check for a connection to an IRC server, bots normally connect to IRC servers on port 6667 (default IRC.)

3. You now have information on the bot server, congratulations, its now time to have some fun or if your just a network admin shutdown this bot network, before logging into the IRC room i suggest you find some information on the bot, the chance's are this bot you have is detected by Anti-Virus programs, if not you can solve this, by mailing it off to all the Anti-Virus companies, here are some links where you can get some information on contacting Anti-Virus companies to send them viruses:

Kaspersky:
http://www.kaspersky.com/contacts

Trend Micro(PC Cillin):
http://subwiz.trendmicro.com/SubWiz/UndetectedMalware-form.asp?TMsessionid=F1862F527EDA4DDEAF07CC9154AFB956&proc=7

H+BEDV(AntiVir):
http://www.free-av.com/images/buttons/contact.htm

Panda Software(Panda Anti-Virus):
http://www.pandasoftware.com/about/contact/

after you have sent the bot to the Anti-Virus companies, you have already accomplished a lot, when you send the virus to Anti-Virus companies you should ask them very nicely if they could tell you information about the bot, they might reply and tell you information about the bot, maybe information about the IRC server and such, if for some reason you were unsuccessful in obtaining it before, the Anti-Virus companies may of found out details about the bot for you.
Now that Anti-Virus companies detect this bot, the chances are the persons bot network will soon dissapear, most of the infected machines are probably running Anti-Virus programs but failed to detect it before, because the bot was no in the Anti-Virus programs database, sending a bot away to an Anti-Virus company can be an effective way of shutting down a script kiddies bot network.
Now if you got a response for Anti-Virus companies they will probably reply to you and tell that that the bot you sent them is a variant of some other bot (often the case), the commands the bot uses will be publicly available, all you have to do is search Google for
Example: Agobot bot commands
Sure enough you should come up with some results, and find information on the bot, now its time to log into the IRC server, open up and IRC client, connect to the network the bot uses and type in
/join #channel password
That should log you in, once in check the names of the bots and log out, if the notice the bots have names like
Bot1
Bot2
Bot3
Bot4

And such, change your name to something like Bot1061
Then login, its a good idea to wait in there, sure enough later on the bot master will come in and be unaware your watching his every move, if you wanted to be very nasty it may be possible to steal his bots by updating the IRC channel they connect to, or sending an uninstall command to all his bots (very few bots have uninstall commands.)
You may wish to log everything the bot master does and threaten to use it against him, if he does not stop attacking your web server.

CONCLUSION:

After reading this information text you should have a brief idea of how Denial of Service attacks work, how to stop them and even how to trace the ones responsible.
Denial of Service attacks are hard to stop when they are happening, the best way to prevent Denial of Service attacks is to make sure the attackers never have the army of bots to attack with in the first place, you can help stop Denial of Service attacks by making sure none of your computers are infected with bots and making sure your network cannot be used as an **Intermediate host** for a DoS attack.

GREETZ:

Greetz to

syst3m of cha0s, htek, TGS, HackJoeSite and The Media Assassins.

USEFUL LINKS:

http://www.securitydocs.com/library/2652
http://www.astalavista.com/?section=dir&cmd=file&id=2164
http://www.securitydocs.com/library/2616
http://www.astalavista.com/?section=dir&cmd=file&id=1705

Aelphaeis Mangarae

DISCLAIMER:

BY READING THIS TUTORIAL YOUR AGREEING YOU KNOW THE AUTHOR OF THIS TEXT CANNOT AND WILL NOT BE HELD RESPONSIBLE FOR ANY DAMAGES ARISING FROM THE MALICIOUS USE OF THIS INFORMATION.
THIS TEXT IS WRITTEN FOR EDUCATIONAL PURPOSES ONLY!
YOU ARE AGREEING YOU WILL NOT CARRY OUT ANY OF THE THINGS WRITTEN IN THIS TEXT, THIS TEXT IS PURELY FOR EDUCATIONAL PURPOSES YOU'RE AGREEING YOU WILL NOT ATTEMPT ANYTHING MENTIONED IN THIS TEXT!