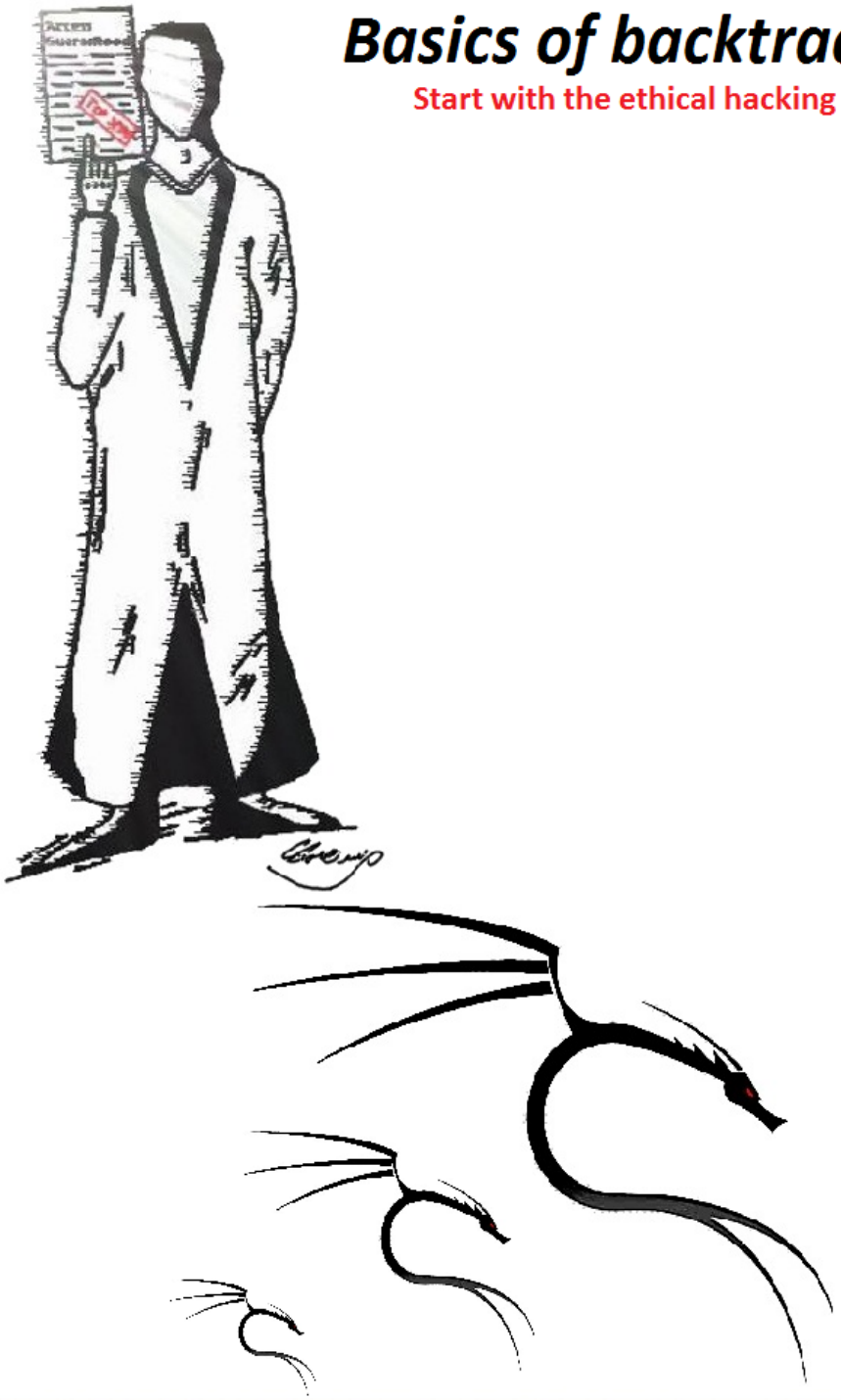
Basics of backtrack

Start with the ethical hacking



I dedicate this book
to my grandchildren.

Index

Preface

Many people know Linux and few people know its true potential. in
this ebook is going to examine all the potential that Linux has to offer an excellent distribution called Backtrack.

I use Backtrack a long time now and again
Today I warmly thank the developers for creating something so wonderfully powerful.
In short, this ebook will guide you to assimilate all those concepts central to using Backtrack a true Ethical Hacker! examining
all those applications that play a key role in this computer science.
Unfortunately not pursue it and go on the very topics of particular everything, so as not to bore the reader or stress less experienced field, so if you wish to explore the topics at the end the ebook you will find useful links to expand your knowledge.
Of course, this document does not require any specific knowledge, In fact the idea is to give a starting point to all those people who
show off their skills in this area and do not know where to start, without neglecting the practical and immediate.
I ask, instead, to experts in the field a little 'to apologize about the topics treated, for you know who, metaphorically, is like making a copy and paste.

Also tend to indicate that the ebook is the result of many, many hours of work and as a matter of personal respect at work I have done, I hope not violated those rights.
Everything you find inside this ebook is the result of my knowledge about this distribution and its applications, gained through study and hard work, and any reproduction or modification document is strictly prohibited.
Finally, I consider that the purpose of this ebook is to convey a basic knowledge on computer security and the basics sull'Ethical Hacking.
E 'to be understood as a document for informational purposes

only, therefore remember that any illegal acts towards others' system, protected or not, is severely punished by law and not justifiable in any way.
The author or ebook are not responsible in any way the actions of others.
Without this essential premise, I hope that you enjoy this ebook and now all that remains is to wish you a happy reading!

If you want to contact me this is my email:
pietro.ciancimino@gmail.com

Introduction to Backtrack

Backtrack is a GNU / Linux created by Mati Aharoni and Max Moser as a distro for information security and penetration testing.
And what will this penetration testing? The penetration testing is that process that takes care to flush out of vulnerability within a system and then, as a result, correct it.

In this final distribution is based on the principle of Computer Security, and any self-respecting hacker should have much knowledge as possible on the subject. The same Keevin David Mitnick, one of the best crackers the world, said the following words: I wish i had many BT 3 years August It would have saved me a lot of time.
This ebook does not examine in detail Backtrack let alone the advanced aspects of pen-testing, but I'll bases and to most useful applications, since this is a world large enough and secure an ebook will not suffice.
Therefore, if this document will be appreciated by many, will be doing possible to show all those elements are missing and the more advanced on the subject, in a second ebook.

Download and install Backtrack

To download Backtrack simply go to the official website: www.backtrack-linux.org/downloads and then click download.
After having pressed the button **downloads** a new page will appear that there asks the features of your computer, or better than the computer where want to run the distribution.
As in the image, the choice is still the desktop environment, the architecture of your processor and the download method.

Chosen your preferences click on "CLICK TO DOWNLOAD" and wait for the operating system from running out.
You have the disk image of Backtrack? Perfect now all that remains is install it on an optical storage medium, such as DVD-ROM or,
even better, on a memory of flash type, such as the USB key.
Now, if you have chosen as a storage drive to a DVD-ROM, just Burn the image using any burning application.
If we want to install the distro on a USB stick, we need only a simple program like **LinuxLive USB Creator** tool totally open-source (free code, and completely free), available from here: www.linuxliveusb.com.
LiLi has a fairly simple and straightforward, which will, in simple steps to install the image of Backtrack on our USB stick.
Without this we will have our distribution Backtrack, ready to use in Within a few minutes.

Prepare the distro

Now that we have our beautiful Linux distribution let's go.
To do this simply insert the drive, DVD or USB, and select from Bios Our computer, the primary boot.
This will be the main screen Backtrack 5, so as we start from photo: **BackTrack Text - Text Default Boot Mode** (start Backtrack default text mode). Booted, you will be asked how to start the distro, there must
startx write the string followed by pressing Enter.
We wait a few more seconds and we will face the distribution, based on computer security, computing worldwide!

Beautiful interface, right? ;) Yeah I know it is wonderful.
Leaving out these details, we immediately set our distribution so as to make it to be operational immediately.
As a first step we will configure the keyboard in Italian, since we will work hard with the Bash shell.
The process is simple, it must go to the System menu, **Preferences**, then **Keyboard**.
Now click on the **Layouts** tab, click the **Add** button, choose how country and **Language** confirm by pressing the **Add** button in the window now select the language and click **Move Up**. Here

the Our keyboard, now, is recognized.
Many applications running on our network card, which require it is configured in monitor mode, without going over the particular **Monitor Mode** is the mode that allows us to see the complete
traffic that is generated within our network.
Programs that require this type of configuration are many, remember Aircrack-ng, which unfortunately in this ebook will not speak, but There will be useful when we go to work with the **Wireshark** packet sniffer.
To activate this mode, type a simple little string in our dear Shell: **airmon-ng start network-name**
Usually, the network name is **wlan0** if we have a collegamente via wi-fi or if **eth0** Lan, but still viewable via the **ifconfig** command.
These two configurations are the most important from the point of view usability of the distribution, but of course you can change all the rest, as the system language, time, mouse, and GUI whatever.

Explore the network with Nmap

Nmap is a tool for port scanning the internet. A port is the point admission, physical or logical, of a connection through which you transfers made between files.
Nmap has infinite utility, we think that most of the vulnerabilities will find them with this small but great tool.
To give some examples, Nmap allows us to know which ports are open or closed on a particular system, or to find out what the
Operating System in use.
The best method of doing this is to send an IP input (Internet Protocol that identifies the network) and commands that want.
To start Nmap must open the console and type nmap. what Support will follow is a list of Nmap, which shows all the commands available with
much of an explanation.
Immediately verify which ports are open on our computer, to do so must be given as input: **nmap-sS (yours_ip)**
and press enter ... we are our beautiful doors open waiting some nice trojan or similar.
Of course this command you can do so with an ip address

differently so as to identify its doors open or closed.
(I remind you that you must perform these tests on the systems you have, otherwise it is a criminal offense)
This small example has stimulated the appetite is not it? And believe it!

Now we'll discover how to identify the operating system of a machine.
Let us then be input:
nmap-sS-O-V (vostro_ip)
The-sS we saw earlier, is used to enable the O-mode OS Detection and-V will also show us a possible version of the system operating.
The table below shows a 'complete list of options available.

EXPLORE THE HOST:
•**-sL**: Scanning a list. Easiest method.
•**-sP**: Ping Scanning. Useful for determining whether a host is online.
•**-P0**: Avoid at all switching host lookup.
• **-PS/PA/PU [portlist]**: Send TCP SYN / ACK or UDP ports indicated.
• **-PE/PP/PM**: Send pacchett standards, similar to the famous ping.

SCANNING TECHNIQUES:
• **-sS/sT/sA/sW/sM**: port scans in general
• **-sN/sF/sX**: Port Scan with outptup of open and closed
• **- scanflags <flags>**: A type of scan "custom"

•**-sO**: Allows you to determine which IP protocols are supported.
•**-b <ftp relay <host>**: Allows you to connect to an FTP server and asks,
Then send the files to a different FTP server.

SPECIFICATIONS FOR THE PORTS:
•**-p <port ranges>**: Scan specified ports Example:-p22;-p1-65535;-p U: 53,111,137, T :21-25, 80,139,8080
•**-F: Fas**t - Scanning only the ports listed in nmap-service
•**-r**: Scanning ports consecutively.

SERVICE / VERSION NOTED:
•**-sV**: Check open ports to determine current services or information
• **- version_light**: Version a little 'more limited, useful for speeding up the
search
• **- version_all**: Try every single probe-packet on every port
• **- version_trace**: Show debugging information about the activities of scanning version.

NOTED OS:
•**-O**: Enable OS detection
•**-osscan_limit**: Detect operating limit
•**-osscan_guess**: Guess OS more "hard"

TIMING AND PERFORMANCE:
•**-T [0-6]**: Set the model of timing (the higher the value, it's fast)
• **--min_hostgroup/max_hostgroup <msec>**: Adjusts the size of groups

for scans parallel
• **--min_parallelism/max_parallelism <msec>**: Changes in parallel
• **--min_rtt_timeout/max_rtt_timeout/initial_rtt_timeout <msec>**: Edit out
• **- host_timeout <msec>**: Stop the search if the host is not respond
• **--scan_delay/--max_scan_delay <msec>**: Edit delays

FIREWALL / IDS EVASION AND SPOOFING:
•**-f, - mtu <val>**: Fragmented Packets
• **D-<decoy1,decoy2[,ME],...>**: Covers a scan using bait
• **S-<IP_Address>**: Soofing entire source
•**-e <iface>**: Use the specified interface
• **-g/--source_port <portnum>**: Use the port number chosen (spoofing)
• **- spoof_mac <mac address, prefix, or vendor name>**: Spoofing
the MAC (hardware)

OUTPUT:
• **-oN/-oX/-oS/-oG <file>**: Output normal, XML, Script Kiddie (XD) and
grepable.
• **<basename>-oA**: Output of all sizes
•**-v**: Verbose Mode (provides more information)
•**-d [level]**: Increase levels or configure debugging
• **- packet_trace**: Show all packets sent and received
• **- iflist**: Show host interfaces
• **- append_output**: Queue output file
• **- <filename> resume**: Resume an aborted scan

Other:

- **-6**: Enable IPv6 scanning with
- **-A**: Enables OS detection and version detection
- **- privileged**: Assume the privileges of Total
- **-V**: Return the version of Nmap
- **-h**: Displays a list of all available commands.

Nmap is amazing is not it? These listed above are almost all commands available (they are missing 3-4 and I have not included because I think they are not very useful).
As we have seen Nmap can do everything and more, by port scanning, identification of the operating system and from circumventing MAC Spoofing the firewall, doors and more.
I remind you that to know the best Nmap need lots of practice ... well as a whole, moreover, is not it?

Swiss-army knife for TCP/IP: Netcat

Netcat, also called "the Swiss boxcutter networks", is one of the most popular tool for information security.
The potential of this small program are almost endless, so to name a few: file transfer, scanning ports, reverse shell, remote administration, banner grabbing and capable even of capture the network traffic. In a few words can make us to netcat everything and more. The only drawback? Creativity!

File transfer

If you can entice even more, every day I use Netcat now;).
In fact just a few minutes ago I had to transfer part of this ebook, the notebook to the desktop (I know, I could use a pen-drive or a cd-rom, but I did;)).
Want to know how I did it with Netcat? It's easier to do that say it! The first procedure is to put in the computer that is listening
would like a free port on a given file (not occupied by any service).
After just take as input, as well as the port number, the name and the file extension you want to send.

Let me give an example, so you understand the process in the best ways:
We simulate a possible transfer, which will be the **Computer_recv** recipient computer and **Computer_send** will be sending computer.
As always, we open our beloved console and **Computer_recv** type:
nc-LVP (port_number)-w (seconds)> (file_name.extension)
example: **nc LVP-6775-w 3> / root / Desktop / document.txt**
Now that **Computer_recv** is listening on port **6775**, let's Computer_send and send in files, typing on his console:
nc-VVN (ip) (port_number) (file_name.extension)
example: ***nc -vvn 192.168.1.8 6775 < /root/Desktop/document.txt***
The file will be sent within a few seconds, then it is obvious that the higher is its weight, the greater the time required.
Here I report the table of options for transferring file;

- **-l**: Puts a system listens for a possible connection
- **-n**: Do not use any DNS system to convert the IP address
- **-p**: port where it listens Netcat (care should be a free port)
- **-v**: The verbose-mode already seen, that will send some information on the process
- **-w**: Limit the maximum time, in seconds.

Port scanning

I had mentioned before that feature of Netcat, you is the port scanning, port scanning properly called.
This we learned that it is already known to Nmap that this is the top, however it may be pointed out useful to be

able to use this
technique with Netcat.
Passing the input, via the console, a single line Netcat will be able to tell us what ports are open or closed:
nc-VVN-z (ip) (range_di_porte)
Example: **VVN-nc-z 192.168.1.8 10-20**
The above example, will tell Netcat not to translate the ip with the-n,
back a lot of information with-vv and make the Input and Output on ports using the TCP protocol. All this ip address **192.168.1.8**
on the doors 10,11,12,13,14,15,16,17,18,19 and 20.
If we want to check this via the UDP protocol and
non-TCP, we must add the-u option to the previous string.
I remember that this process is quite slow and will certainly require a couple of minutes, however it is really worth having the amazing
results.

Remote administration

Another noteworthy feature is the ability to upload to a Netcat files with the extension **.exe** (an executable so from Microsoft Windows) and redirect it to another system favoring remote administration, also the entire system.
Note: This is a very dangerous if used incorrectly
can also cause loss of file system, so as to compromise
the entire computer.
Without this little detail, let's see how it works.
As always we will simulate two computers;
Computer_back is your **client** that will execute the file. Exe.
Computer_win will serve as the **server** computer, which directs the file **.exe** the **client** computer.
(On Computer_back course runs Backtrack the distribution, while Computer_win runs on any Windows operating system)
We go on our **Computer_win** and we start netcat. (Obviously there The program will Netcat for Windows, downloadable at: www.downloadnetcat.com). Once we started the following line:
-v-lp (port_number)-and cmd.exe
The first 3 options already know them: the option-v is verbose mode- (shows information about the process), l-a connection and starts listening **-p** specifies the desired port. Also there is

the fourth option,**-e**, which
this case, your task is to perform a particular file
.exe.
Now our server is listening to establish a connection.
The interface is that you should look like this:
So we're going to connect to the server (**Computer_win**) through our client (**Computer_back**), typing on the console the following line:
nc-vv-n (ip) (port_number)
We already know all the options so I will avoid just used to rewrite all, the cycle will generate is quite simple: we ask for Netcat
connect to that ip and port indicated.
If you did everything correctly, you have established a connection between the Computer_win and Computer_back that will allow you to run the prompt command on the server computer, on your distro Backtrack.
In short, you have almost total control of Computer_win.

An instant chat

Modestly speaking, I used this method very few times, but can sometimes be used to establish a communication channel through this chat, which by the way is anonymous and does not leave any trace on computer.
To initiate this communication channel will need two computer. First we go on first and let the console:
nc-l-p (port_number) (I remind you that need to connect the IP address of first computer, from Windows to get it type: **ipconfig** from Linux: **ifconfig-a**) Now on the other computer dates from the console:
nc (ip) (port_number)
These are just some of the potential that enables us to netcat available, there are many options waiting to be explored.

Wireshark

Wireshark is a tool that can analyze network protocols and to perform the so-called **packet-sniffing**. Packet-sniffing is that activities passive interception of all data traveling over a network.
All software products that offer these activities are called **Sniffer** and Backtrack are the famous and powerful: Wireshark.

Also this application can boast about having a simple
and intuitive graphical interface that will allow us to order so
correct and understandable way the captured packets.
In short a sniffer can capture all the information that
sailing in a network and route them back to us.
Let me give a simple example: Luke has a laptop and connects
to wi-fi at home, his brother Mark uses that network and
connects to it through a desktop computer. Luke and Mark visit
various websites, some suspicious, and wants to know what
sites you visit the little Luke, then opens Wireshark, set up
various filters and starts capturing packets
circulating within the network on the computer of Luke.
Mark instantly get real-time list of all websites
visited by brother Luke, without the latter's aware of it.
(Note: before starting Wireshark it is essential to enable
monitormode of your network card (p. 13))

Hunting for packages

We go now to start **Wireshark** to do so simply run the
program from the terminal: wireshark.
(Note: Wireshark needs to be started with full root privileges)
Once launched we will present a window similar to this:
To begin to **capture** information will need to click on the menu
Capture **Interfaces** and after.
At this point you have to select your network interface, one that
we have previously set as a monitor-mode and set properly the
various options on the **Options** button.

When you are ready press the **Start** entry, and do well from the capture process. We find something similar ...
Now we can do is wait a few minutes and find the window invaded all sorts of packages, each package corresponds to an entry other than identifying it with: a number, the time taken, its
origin, destination, protocol, and small details.

Just browse through the packages to find one that interests us. On the next page, find out how to narrow our search
The Capture Filter (a kind of filters that restrict the packages without much confusion) so as to quickly find what they seek.

Filter out the research

As we saw earlier, if we do not specify what to Wireshark we want to achieve, he catches everything and this certainly is not conducive to maximum. In certain situations there is the need to seek particular protocol or, even better, a goal "dry" as a website or similar. In this Wireshark does not leave us alone,

indeed, helps us with our **filters special** permits us to analyze traffic within a given network, leaving out the "junk".
To set a filter you need to click the button in the **Capture Filter Capture Option** window, view a short while ago, and specify the type of filter we want to apply.

Those available are;
Ethernet address: To specify a specific MAC Address
Ethernet type: specifications for the ARP
No and no multicast broadcast: Broadcast does not accept and / or Multicast
No ARP: ARP does not accept
IP only: returns only the IP
IP address: returns the packets to the IP address specified for
IPX only: returns only the IPX packets
TCP only: returns only TCP packets
UDP only: returns only the UDP packets
TCP or UDP port 80 (HTTP): returns only the packets related to TCP and UDP protocols that operate on port 80 (HTTP, the usual sites
web)
HTTP TCP port (80): returns only for TCP packets,
Port 80 (HTTP)
No ARP and no DNS: does not return the packets of ARP and DNS.

These filters listed above are present in our application,
we could also create our functionally similar or
totally different, simply click the **New** button.
Once you choose the filter you want, just double click on it or select it and click, then click **OK**.

Operate on secure networks

If you own a secure wireless router has just realized that he did not appears none of it. This is because Wireshark is not able to perform scans over a secure network, so we have
set the router password on our beautiful tool.
Come on then click on **Edit** and then **Preferences**, here spuntiamo voice Protocols and select **IEEE 802.11**. At this point the box select **Enable decryption** and enter the password of your router on the item **Key # 1** and confirmed.
Now you will be able to use Wireshark also think that you, wisely, secure your network.

Cracking of password

Passwords can be used as a method of authentication systems or areas reserved for user data.
When a system to provide a username (nickname) and password he shall consider, if they find the right combination will allow us access.
Otherwise the alternatives are not many ... or we already know or ...

try to get it.
In the following section we will find out how you can crack password in offline mode. That all those passwords which are usually located within the local limits of the system.
For the password cracking process can mean that decrypt a string or the like, previously encrypted with the intervention human or machine.

John the Ripper

John is a tool used to crack the password hash. At the moment is able to crack more than 40 types of password hashes, some of them are: MD5, LM NT, Crypt, NETLM and DES.
To view the help of John, just take a shell: **john**.
While I recommend you do to start it manually via the **menu**, then **Application, Backtrack, Privilege Escalation, password Attack, Offline Attacks,** and **John the Ripper**.

Now we take our password hash and paste it into a text document. Without this we can from the console, previously opened, the following string:
john (destination file name extension)
Example: **john / root / Desktop / file.txt**
If the password is included in the root folder of files **password.lst** of john, you will discover for sure.
(Note: It is recommended to add items to the list of passwords of John, so ensure greater success, in order to find the password. To do this just go to the folder **pentest**, present in the **root** directory, exploring the folder **passwords**, and then go to the **john** folder.
Here you will find a file called **password.lst**, this is file is a word-list (word list) and this is where you need to add more values)

Crunch – the origin of a Word-List

Crunch is a tool that allows you to generate a word-list. as already know, the word-list is used in the brute-forcing tools, such as John the Ripper, to find the correct password.
Crunch is not installed by default on Backtrack 5, so you have download.
Once downloaded, you just give to console **crunch**, to view the help, while if we want to create a word-list, do as follows example: **crunch 1 4-f lista.lst lalpha-numeric-or wordlist.lst**
With the above example we will create a one-word list Alphanumeric, 1 to 4 characters, which will be saved in the file **wordlist.lst**.
Now that we have our word-list, we move to the brute-forcing with a of the many tools available to backtrack. My advice is to use the now famous John the Ripper!

Acknowledgments

Thank you very much for purchasing this ebook.
I hope very much that there has been helpful and that somehow there has opened the doors to this wonderful journey.
Remember that negativity only brings more negativity and I think that nobody likes that, therefore, used these little pills on security wisely and remember that to violate a system others is an offense that is prosecuted.
Warm greetings from Pietro Ciancimino.

(I used a program to translate the following text into English, I apologize for any inconvenience)

The more a system is safe,
more is unnecessary.
Pietro Ciancimino