# The Way of the Blackhat

Made by ‘Unobtainium’ of www.hackforums.net

Also known as ‘Devil Touch’ in a past life :P

“ 2 + 2 = 5 ”

## | Chapter 1 |

## Knowledge

First things first, we all must understand that a good hacker never stops learning. This applies to much more than software and hardware knowledge. Although keeping up with technological progress is already a huge task, a good hacker must also take care of his ‘second personality’. Right now you must be wondering “Second personality… WTF?” ; “Hackers have schizophrenia?” ; “Is the author on crack?”. Well, to clarify on this point, we must see hackers as having two sides.

One side is the ‘good boy/girl’ side that you show off in society (school, work, etc.). This side can help the other one which is the ‘bad boy/girl’ (that you only show off with trusted people, hacking networks, etc.) by doing social manipulation [social engineering] – *see | Chapter 2 | for more information on social engineering.*

With these two sides comes a ‘priority of operations’. This means that one side is more important than the other and takes over the other in certain situations. The more important side is the ‘good boy/girl’ side. For example, if you’re in class with trusted people (people that know about your ‘bad’ side) you should NOT give any clue on your true personality whether it’d be by talking about your activities, actually hacking the teacher’s computer, etc. The funny fact is that the side that makes a hacker who he is is usually kept secret. This is done, mostly, to assure correct and working social engineering.

### Pattern draw:

Fake ‘good’ side = gathering important/somewhat sensitive information from people

Real ‘bad’ side = exploit/abuse/take advantage of the information gathered to obtain private/extremely sensitive data (CC, bank accounts, online accounts, etc.)

As we all know (I hope), technology evolves rapidly, even more since the last decade. This means that new hardware and software are implemented in mainstream computers (the computer of your average Joe) every few years. One thing most hardware makers make sure of when releasing a new product on the market is guaranteed product's stability. In order to make a hardware piece stable (safe from crashes/destruction) good software must back it up. Hardware does not go without software and vice versa. This is an obvious fact, but it's at the core of machine hacking.

To keep up with software advances is a very hefty task. It is so, because most archives of software updates on the Internet aren't well organized and most companies publish limited information on their releases. Another reason behind this is the fact that there are a lot of developers out there. A LOT of them. As far as I know, there aren't any statistics out there on the subject, but I'd say the ratio of software developers to hardware developers is 1000:1 (probably even more – I wouldn't be surprised). Now, the reason behind software developers being more popular is a social tendency. All this to say that the trick in keeping up with technological evolution is to follow the hardware evolution. Companies provide full information about their updates to existing hardware, new releases, etc. There is no reason in keeping it a secret because reverse engineering exists and it can provide all the details of a new piece of hardware. You might say "Reverse engineering exists for software as well!". That's very true, but it doesn't get you very far.

By reading about new hardware development, you also are referred to associated software development. Archives usually link software updates (called firmware updates when they are implemented in hardware directly) to their released products. This makes it easy for you to be up to date with the new 'security' measures.

Let's take the popular routers made by Linksys as an example. These come in play when trying to hack your neighbors wireless network key (WEP/WPA).

Their support website (http://homesupport.cisco.com/en-us/wireless/linksys) gives you access to any of their router's firmware updates/release notes/etc.

In conclusion, a hacker must be well aware of his actions and must be up to date with the latest security software found in mainstream computers.

# | Chapter 2 |

## Social manipulation [engineering]

Social engineering is done by everyone, not only hackers. Most of us don’t even realize we do it. It’s something that is somewhat subconscious if not done abusively. When we want something very badly, our brain works to understand how people that can potentially get us to our goal function. By understanding these persons in a better way, we are able to manipulate them to achieve our goal. Manipulating people can go from saying a few words to elaborating a whole scheme to gain their trust. It can be a piece of cake, but it can also be a pain in the arse. The difficulty of manipulating someone varies according to a huge amount of factors. Here are some of these factors:

- How much do you know the person (the more you know the better);
- How much does the person know you (generally the more they know, the worse);
- How much does the person trust you (if the person doesn’t trust you, you need to earn their trust before proceeding to manipulating);
- How gullible is the person (the more, the better – obviously);
- How aware is the person of what you are doing *;
- How kind is the person (you obviously want to fall on a very kind person).

- The list goes on and on -

* This applies to the most common kind of manipulation – information extraction. When you want to extract information on a person’s machine, you have to do it very subtly or else the person might realize your plans. It doesn’t really apply to other kinds of manipulation – such as getting someone to buy something for you – because they are mostly aware of what you want but are convinced in doing what you want.

Here is a brief example of social engineering:

Goal of the hacker: Get into the target's computer

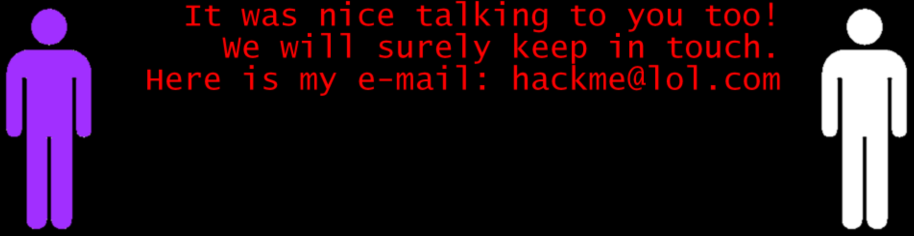
- Introduce yourself and make small talk -

I got a new computer last night. I can't make up my mind as to what operating system I should install. What operating system do you use?

Oh, well I use Windoze. I really love it. It's the most secure OS ever!!!

- Continue making conversation –

Oh damn! I haven't seen the time fly by so fast! I really have to go. I enjoyed talking to you. I'll give you my e-mail so we can keep in touch.



It was nice talking to you too!
We will surely keep in touch.
Here is my e-mail: hackme@lol.com

– You leave with few information, but enough if you are an experimented hacker –

You have his OS and his e-mail address. You can get his IP address either by IM or by receiving a simple e-mail from him and checking the e-mail's source. Once you have his IP address and you know his OS, you can exploit (metasploit, etc.) – *see | Chapter 3 | for more information on basic hacking tools* - and gain access to his computer [†]. Once done, your goal is achieved.

Oh no! Someone hacked my computer!
My online banking account got
4'000'000 $ taken out of it!
Who could have done this?!
:(

[†] This involves using software applications such as *Nmap* (port scanner), *virtual machines*, *metasploit* (host software exploiter), etc. Social engineering helps you in your software usage.

This is obviously a basic example of social manipulation – more precisely, information extraction. In this case we haven't manipulated much, but sometimes that's all we need.

You might wonder "Is it really moral to be a social engineer?". Of course NOT! Actually, it depends on who you are. Since everyone is a social engineer and everyone manipulated someone at some point, we could consider it perfectly normal and moral. Although, some persons abuse it and manipulate people all their life. In this case we could consider it being immoral. But, some people consider it moral, because they put the blame on the people being manipulated (saying they are too blind).

The fun fact is that experimented social engineers could change the face of the world for the better. Since they have a 'gift' to convince people to do things for their own benefit, they could convince people to do thing for the world's benefit. Yep, they do have a big influence. Just as an example, a social manipulator could convince someone to donate money to charity. But, of course, once you are able to do that, you only think about yourself and about the big money YOU could get.

In conclusion, you and me are social engineers. We can develop our engineering abilities in this domain simply by practice and study of our entourage.

## | Chapter 3 |

## Basic ‘must-have’ hacking tools

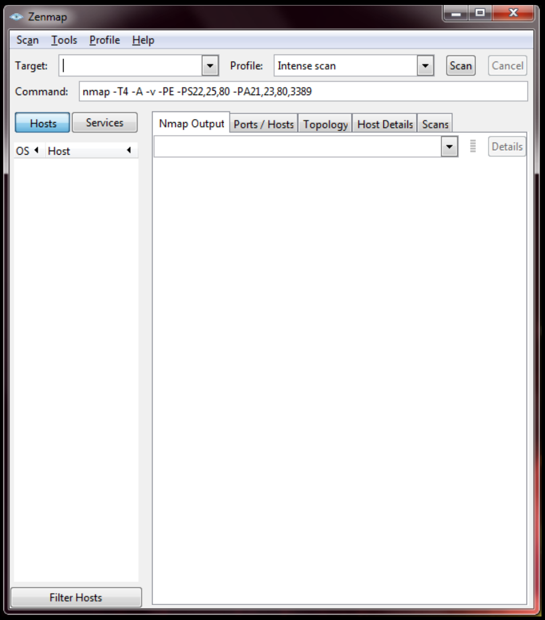
This section is dedicated to software commonly used by hackers and what their purpose/utility is. A brief description will be given, since I do not want to make this eBook 200 pages long :P. *This section doesn’t follow the philosophical intent of the book, but I feel it necessary to give out the basics.*

*~ Yay! No more bla bla… We finally get something worth our time! :P ~*

*Nmap:* Download link: http://nmap.org/download.html

Nmap is a ‘security port scanner’ that finds vulnerabilities in machines. It detects running programs on certain open ports of the targeted computer and gives you detailed information on the program in question. With this tool alone you CANNOT gain access to someones computer. You need to pair it up with an exploiter such as *metasploit* (that will be our next subject).

Interface screenshot:



Target:

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389

*Metasploit:* Download link:

http://www.metasploit.com/framework/download/

Metasploit is a command-line based ‘framework’ (as they like calling it) that shows you and lets you use dozens and dozens of public and somewhat private exploits. There are exploits for Windoze, Linux and Unix OSes. Basically, you take the vulnerabilities you found with Nmap and exploit them with *meta*.

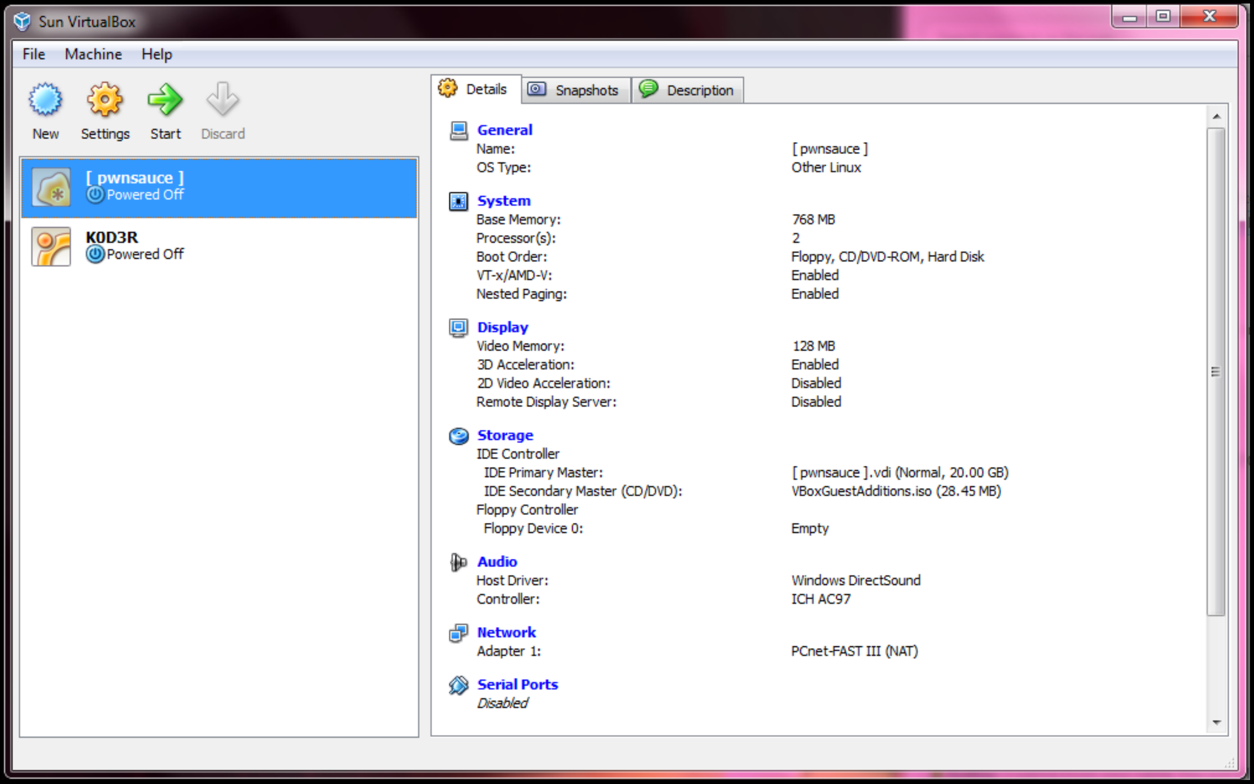
*No screenshot as it is command-line (meaning the interface will be your OS’s console)*

*VirtualBox:* Download link:

http://www.virtualbox.org/wiki/Downloads

VirtualBox is a free open source virtual machine creator. Get rid of the overrated VMware :P. At the base this does the same thing as VMware except it doesn’t require you to crack it because it’s FREE! This will allow you to run a second OS at the same time as your main OS. It creates a guest OS and you can control it at the same time as your controlling your main OS. Very useful when you want to be able to erase sensitive data that you acquired while hacking (whereas if you did it on your main OS, you’d probably have to cook your hard disk to destroy all evidence).

Interface screenshot:



```
General
Name:                                   [ pwnsauce ]
OS Type:                                Other Linux

System
Base Memory:                            768 MB
Processor(s):                           2
Boot Order:                             Floppy, CD/DVD-ROM, Hard Disk
VT-x/AMD-V:                             Enabled
Nested Paging:                          Enabled

Display
Video Memory:                           128 MB
3D Acceleration:                        Enabled
2D Video Acceleration:                  Disabled
Remote Display Server:                  Disabled

Storage
IDE Controller
  IDE Primary Master:                   [ pwnsauce ].vdi (Normal, 20.00 GB)
  IDE Secondary Master (CD/DVD):        VBoxGuestAdditions.iso (28.45 MB)
Floppy Controller
  Floppy Device 0:                      Empty

Audio
Host Driver:                            Windows DirectSound
Controller:                             ICH AC97

Network
Adapter 1:                              PCnet-FAST III (NAT)

Serial Ports
Disabled
```

- In this version (yes I will make a V2) I will only 'give out' these three programs as the main hacking programs –

There are hundreds maybe thousands of different goals when hacking. These programs can't cover all the types of hacking. This time, I decided to cover the basics on the most popular kind of hacking: hacking another machine.

## / HackForums links to useful hacking tools and threads \

*Note: These links may go down in time as threads on the forum get deleted

∞ RATs/Keyloggers/Stealers *by Anubis™*

http://www.hackforums.net/showthread.php?tid=595859

∞ Index of hacking tutorials *by Valiant*

http://hackforums.net/showthread.php?tid=504268

∞ List of MD5 web crackers *by th3.g4m3_0v3r*

http://www.hackforums.net/showthread.php?tid=591358

∞ Crypters/Binders/Virus Builders *by flAmingw0rm*

http://www.hackforums.net/showthread.php?tid=238890

∞ Security programs *by protocol™*

http://www.hackforums.net/showthread.php?tid=592772

∞ Ultimate guide to PC Security *by Vaqxine*

http://www.hackforums.net/showthread.php?tid=34240

∞ Hack a Gmail account *by Encrypted32*

http://www.hackforums.net/showthread.php?tid=572968

∞ Botnet setup *by Legym*

http://www.hackforums.net/showthread.php?tid=101297

∞ Wireless network hacking *by D00MR4ZR*

http://www.hackforums.net/showthread.php?tid=502252

I hope you enjoy!

Notify me if ever one of these links goes down/changes and I will gladly update it.

# | Chapter 4 |

## The Brotherhood

### 0. Intro

This chapter is dedicated to hacking communities and the people that are found in them. Hacking communities are places for hackers to share their knowledge and progress. Most often, the communities allow any hacker to enter – whether it'd be the extremely advanced hacker or the beginner 'n00b' hacker. If you are a beginner, do not hesitate to ask around, although not too much :P. People are there to help you and, if you ask politely, you will more than certainly get an adequate answer.

### 1. Rules

Hacking communities, as real-life social communities, have rules you must obey to. They are common sense rules that make the stay at the community more pleasant [such as NO SPAMMING]. "I thought hackers were free to do whatever they wanted." It's partially true. Even hackers are limited in their actions. If they wouldn't be, the Internet would be chaos. Furthermore, they are free to break the rules, but they will have to suffer the consequences of doing so.

There are users (usually users that don't have much hacking experience) that join a hacking community just for the heck of breaking the rules and pissing everyone off. For example, HF has a rule forbidding users to post a infected files. This is done to keep the hacking level between members to a minimum. There has been, although very few cases, persons who joined and posted infected files for users to download, saying it was a good hacking tool.

Usually new users (with low post count when it's question of a forum) are suspected of breaking rules/scamming others/etc. It's a very normal way of thinking. This is an auto-protection measure that you have taken all your life and will continue taking. Remember when your mummy told you "Never talk to strangers"? Well, this is exactly a 'stranger' case. Nobody knows much about the new user and therefore, he is a stranger. We never trust strangers. Although, everyone has started off as a new user at some point and progressed out of it. This to say that new users should at least gain a certain respect from other members. Not necessarily their trust but at least their respect. A lot of ‘older’ users treat new users badly because they associate ‘stranger’ to ‘no trust’ and ‘no trust’ to ‘not worthy of anything else either’.

## 2. Community vs. Community

Some communities hate other communities for the reason being that they copy most of their content (without crediting most of the time). This provokes endless flaming wars and leads to an eventual DoS/DDoS of one of the community’s website. The website that remains up is declared ‘winner’. Although, as I have had the opportunity to see this a few times, the remaining community is soon to be DDoSed as well by the others. In the end, nobody wins and it’s just a waste of time and keystrokes. The solution to this is to not care about other communities’ work/actions and to take care of OUR users. This way, we are the ones being promoted.

~ More in v2

## | Up Next |

## Plans for v2

- Programming languages information/tutorials/links;
- More information on the past 4 chapters;
- A section reserved to in-depth hacking tutorials;
- More pictures to ease the reading;
- A section reserved for game hacking;
- A section reserved for interesting Open Source ‘free’ programs.

*This eBook was more of a tease compared to the upcoming one. Everything I produce will be kept free!*

*I hope you enjoyed!*

Disclaimer: I do *NOT* recommend doing any of the above. Everything stated in this book is for informational and educational purposes ONLY! Use at your own risk.

If you have any questions or suggestions I would be more than glad to hear what you have to say and help you! Just PM me on HF.

*Note from the author:*

The reason I made this eBook free is because I believe in free access to information and promote and support open source, free applications!

~ Believe in free access to information ~

~ Believe in Open Source ~

~ Believe in theoretical Communism ~

*SOON TO COME – V2*

*WITH MORE INFORMATION AND MORE BANG FOR THE HACKER*