Security Penetration Testing Loves “Free Software”

Fernandez, Christian
ReK2,ReK2WiLdS
Hispagatos, Bugcrowd

Troy Cregger
Trizz
Hispagatos

_# WHOAMI

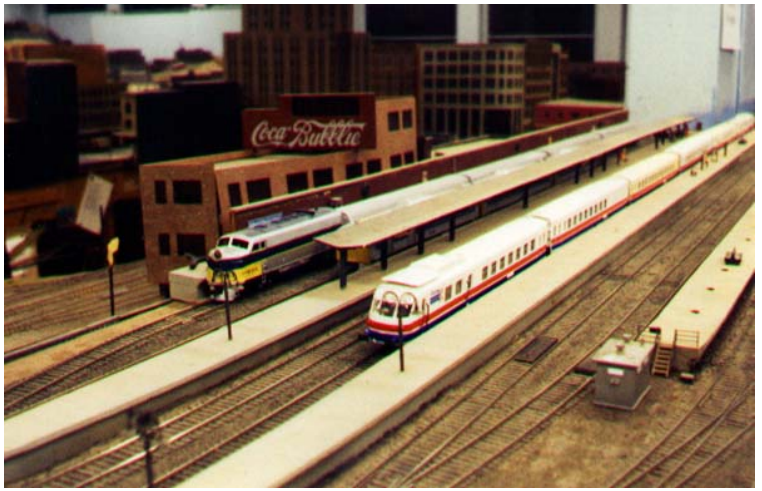
Currently working at: ***Bugcrowd*** *as a* ***Infrastructure and Security engineer****.*
Originally from Alicante, Spain, A ***Free software advocate*** *since 1996,* ***Anarchist***
An ***autodidact****, am mostly self taught. Companies, do make me take certifications for Compliance… which is ok.*

Back in the day I loved to play all night on BBS's finding hidden underground information, Hunger to learn as much as I could, something my mother did not really understand when the bill came at the end of the month…
Then FIDONET and just soon after the INTERNET, where I used to connect using compurserve from Spain in not very ethical ways… but Telefonica was a company I was not willing to give a dime or a peseta at the moment.

Groups:
Hispagatos
DC415

Employeer:
Infrastructure and Security Engineer
at Bugcrowd in San Francisco

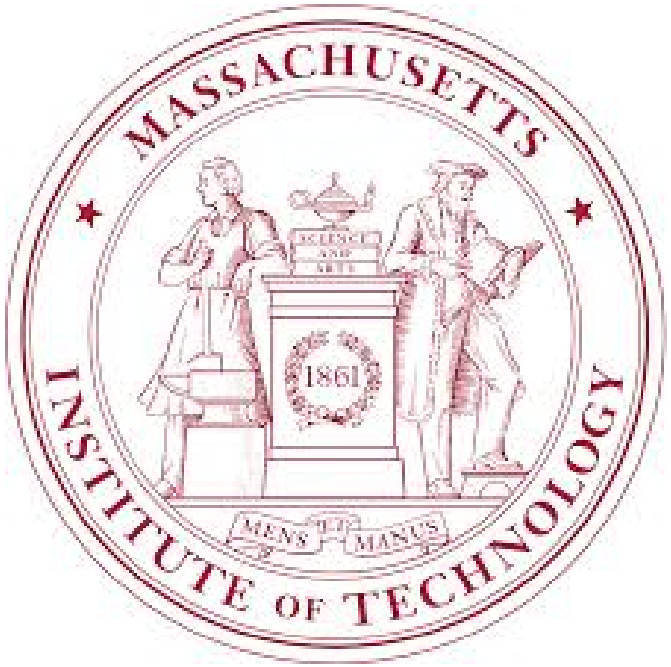
Freelancer:
Stealthy-cybersecurity
Penetration testing and other security services.



And it all started…

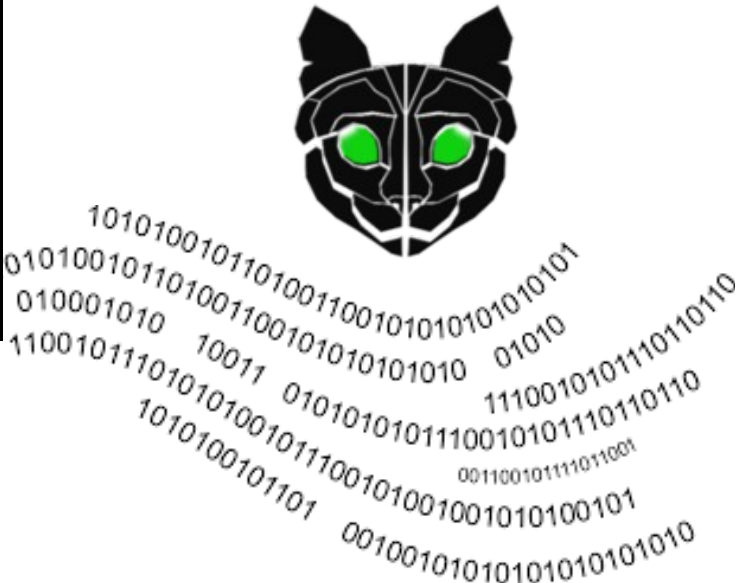
and.. yes

as we know it today, it all started in MIT with some clever people playing with raildroad models…



A new frontier...

Cyberpunks, explorers and other technocrats started to roam the wild wild west of what was coined by Willian Gipson at the time as "CyberSpace".

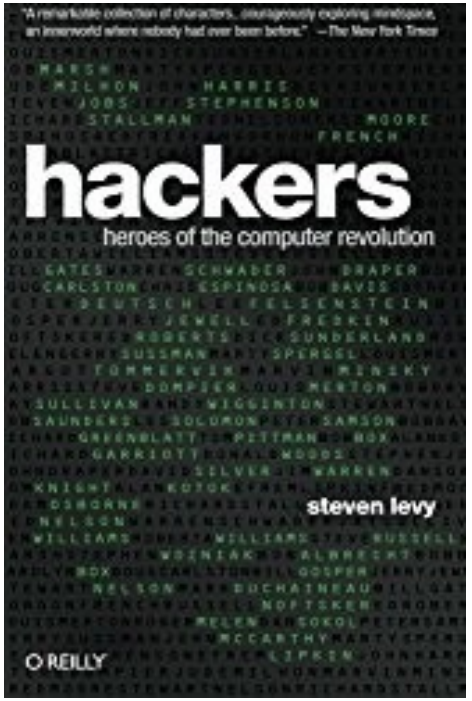


The seeds of change...

Richard Stallman started the GNU revolution,
around the same time
the LOD or Legion of Doom and MOD also known
as Masters of Deception were exploring
this decentralized new frontier.

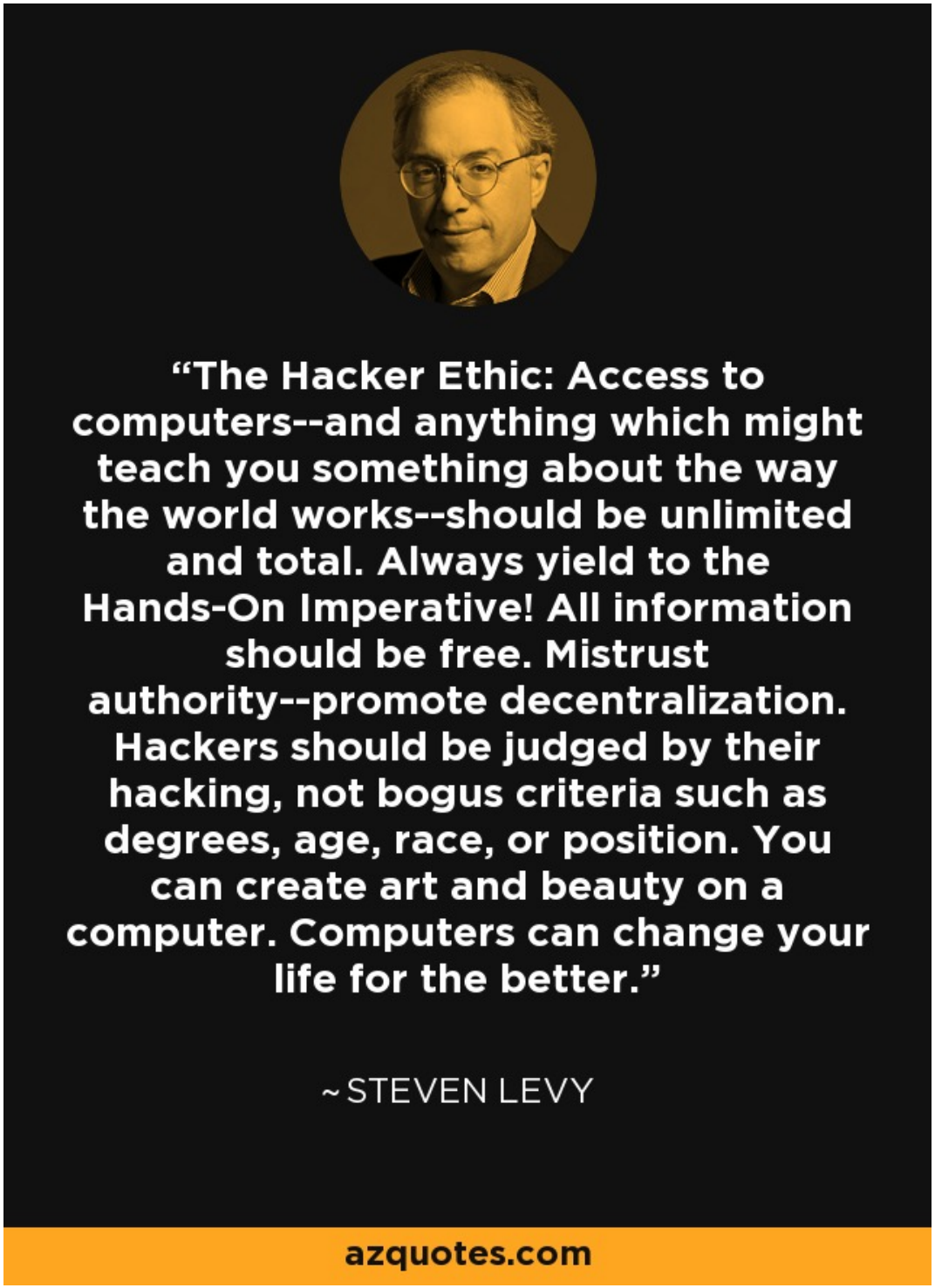
Both movements, making old power structures nervous in diff ways..

“Hackers”, Heroes of the Computer Revolution:



Steven levy

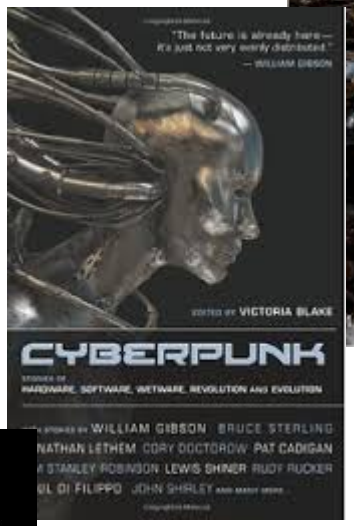
Gracefully documented the great hacker tradition for many decades to come…



The hacker Ethics

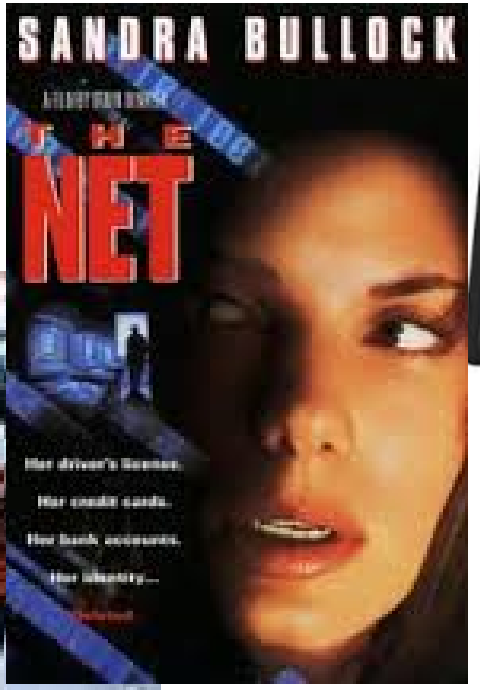
Set in stone, for the comming generations and an array of movements that came out of it

Just to name a few influencial movements:



Ok, so looks awesome.. seems we are on the right path, right?

Well...
then this happened

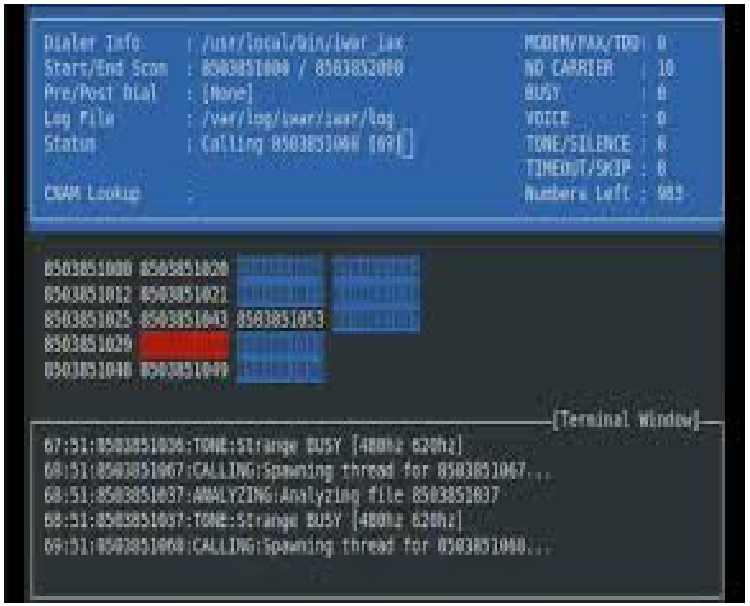


That and the media... this was the total assimilation of the word “hacker” in a negative way...
that's just what we needed... NOT.

And in the Free Software camp also a lot of campaigns to discredit its model and ideas.

Still, there were real hackers in both communities... the software hackers and the computer hackers, and this is what this talk is about...

Both of these communities were and probably are the same community, the tools people use for security for the last 20-25 years were written by software hackers for computer hacking and security.



hping

Such software, of course, respected the hacker ethics and was released as free software in most cases or other compatible licences.

So here we are.. hand by hand Free Software and Computer Security

The moderm computer security field needs hackers to write software that is open, free and respects the hacker ethics while at the same time breaking and going beyond what we can expect as is usually done in the true hacker spirit.

Now lets forward to 2010, Computer Security is getting to be a big bussiness, hackers are in demand, new tech fields are created over traditional ones. Security Engineers, Pentesters, Blue Teams, Red Teams...

Pentesting is to computer hacking what Open source is to Free software...
Stripping the politics and idealism out of them to create a simpler pro-bussiness market easier to digest.

So yes here we are. Now we have a lot of academics non-hackers doing pentesting and security. In the last 5 years security is a multibillion dollar market, a lot of software companies are trying to get a piece of the pie. This is ok, but what about the hacker ethics? What about the freedom and the open decentralized ideas of the hacker revolution by Steven Levy?

This talk is not intented to agree or disagree or discredit any profesionals, but to be able to talk about why free software is needed in the penetration testing world. We have to know the link between the past and the present. So from now on I will describe hacking as penetration testing...

Pentesting & FreeSofware

It took a lot of time for people to understand and fully respect the whole point that open and libre are not a threat, but will actually revolutionize the internet era...and so it did. The same with security hackers, it took 20 years for people to understand the difference between people exploring and pranking. The difference between curiosity and real criminal behaivour. Today we are hired and not demonized. Others were not that lucky...

Popular software that hackers have written along the years that are used by security profesionals, some of them are:

Nmap
OpenVas
Hydra
Netcat
Ncat
Nikto
Hping
Gdb
gcc
Zaproxy..

Long list..

So…. What's the problem? Most tools are free sofware..

Like we said before… as the hacker ethics leave the field also does free software, a lot of new professionals already abandoned free software options, they use tools like BURP, comercial and closed tools made by the evolving market that are in most cases closed source.

Sometimes… is really not their fault, some propietary tools like BURP have come a long way with no free competition, and these people don't care about freedom until OWASP stepped in… now we have ZAProxy… but even though it got much better in just the last 6 months, it still needs more people collaborating… and for us to spread the word so other pentesters will use it

Ok let me now give you an over view of the tools I usually use when I am engaged in a pentest.

My main tools:

Lots of custom ruby, python and golang scripts/programs I write.
Some ruby examples I put along other collegues at:
RuByFu Gitbook

Linux(BlackArch)
Nmap,Ncat,Hping
The-backdoor-factory, Veil Framework
Zaproxy, Nikto, WPscan
Gdb/peda,radare2/ragg2,GCC
Recong-ng, pwnbin, google dorks
Spiderlabs/Responder, smbtools, Enum4Linux
SecLists/dictionaries, lots of personal notes.
Tcpdump/wireshark...
Sqlmap/metasploit...
Aircrack/wifite2/mitmf...
Snmpwalk...

VirtualBox:

I have a repository of VM's with propietary OS's to attack and to compile exploits for win32 enviroments etc. Unfortunatelly this can't be avoided... since you have to experiement attacking these systems, just make sure they are VM's not your main OS :P I treat them like viruses I need to study :P

Radare2/x64_dbg/objdump/nasm/edb/

Methodology

- Information Gathering

Recon-ng, google, bing, duckduckgo, nslookup, dig...

- Enumeration/scanning, detect live Hosts,Ports etc.

Nmap, ncat, hping,Snmpwalk,enum4linux...

- Sniffing and MITM attacks if possible..

Mitmf, tcpdump, wireshark, responder

- Exploitation

--getting-shell:

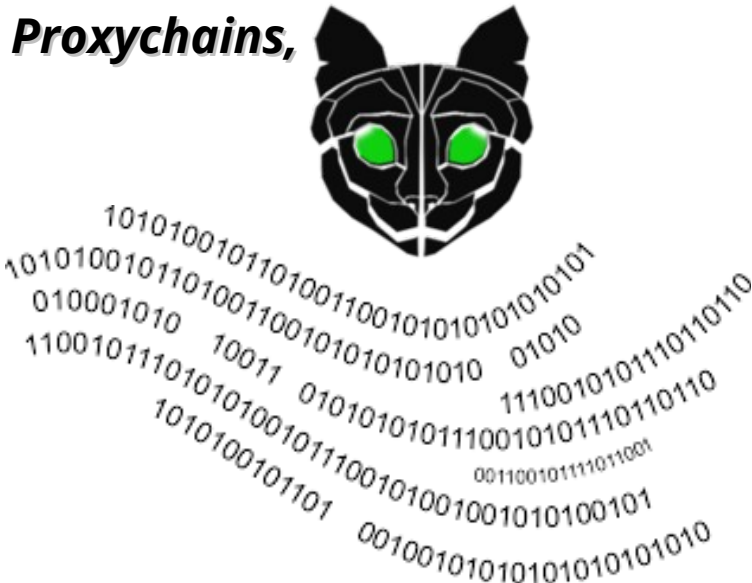
Custom made exploit, Veil framework, exploit-db.com, Proxychains, ssh, telnet, ncat, ftp....sqlI,XXS,phising...

--Privilege scalation:

Local exploits/vulns, bad permissions, misconfigurations

- Post Exploitation

Pillaging, mapping internal network, pivoting, repeat



Thanks to my team members at Hispagatos

Trizz, Thibaud, Bitsurfer, sigma4, Heavenraiza, Petruknisme

http://hispagatos.org

We use mattermost chat if any of you wants to join the chat ask me for an invite, anyone is welcome

How to Reach me?

I am always willing to help people starting, specially if you are an anarchist or a free software activist.

KEYBASE: https://keybase.io/cfernandez

Email: rek2@protonmail.com

Email:cfernandez@protonmail.ch