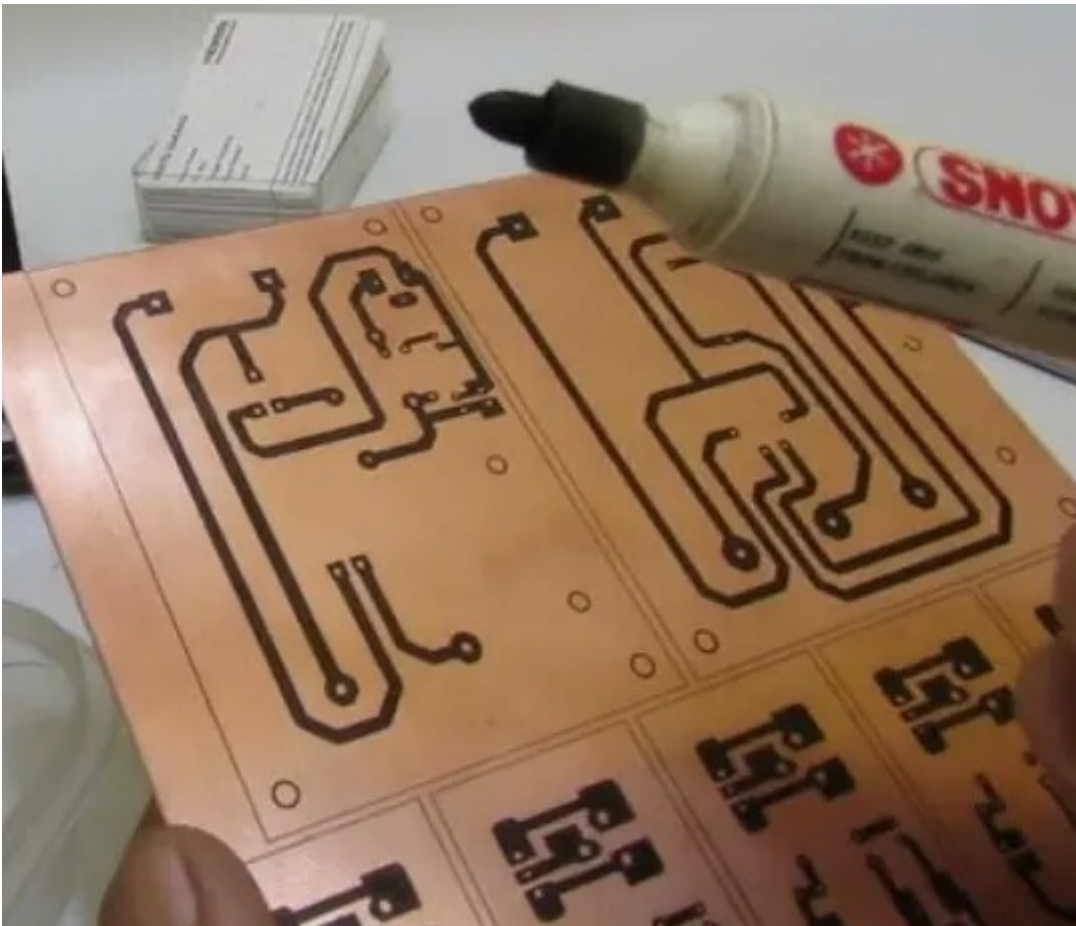


Young Body – Old Soul ! A Long Journey !

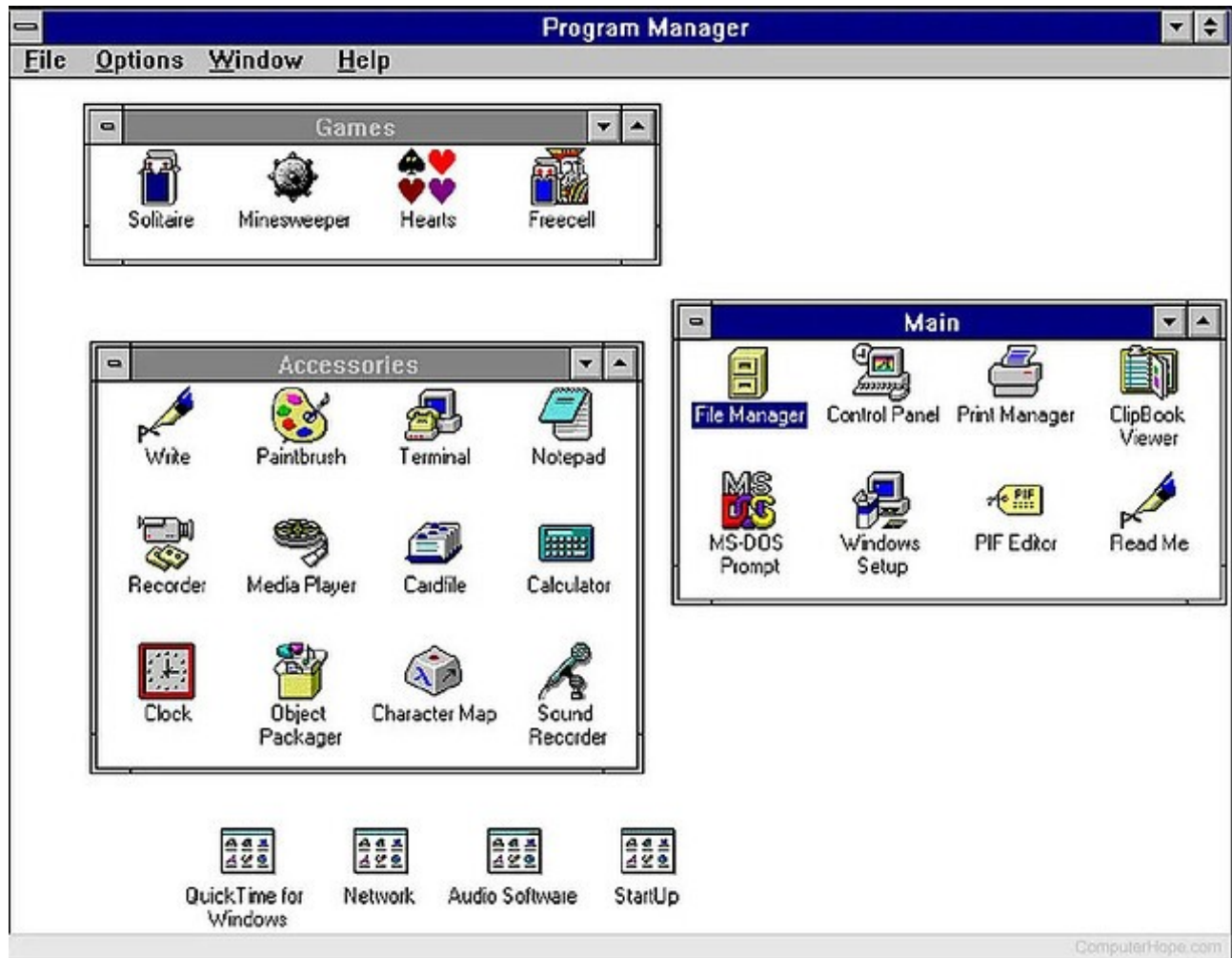
The following is the story of how I came to know the world of hacking !

Before Discovering Computers



Going back to 1996, when I was still in school, I was introduced to a new extracurricular activity: electronics. At that time, I learned how to make printed circuit boards (PCBs) using ferric chloride and marker pens, how to solder, and the fundamentals of electronic schematics. Things were not as easy as they are today — I had no knowledge of PCB design software because I had not yet encountered computers, so everything was done manually.

First Encounter with Computers



In 1998, I gained access to another new extracurricular activity at school: an introduction to computers. At that time, what I studied included MS-DOS, Windows 3.x, Windows 95, Windows 98, Lotus 1-2-3 (a spreadsheet application similar to Microsoft Excel), dBASE III Plus (a database application similar to Microsoft Access), and WordStar (a word processor similar to Microsoft Word).

A	A	B	C	D	E	F	G
1	EMP	EMP_NAME	DEPTNO	JOB	YEARS	SALARY	BONUS
2	1777	Azibad	4000	Sales	2	40000	10000
3	81964	Brown	6000	Sales	3	45000	10000
4	40370	Burns	6000	Mgr	4	75000	25000
5	50706	Caeser	7000	Mgr	3	65000	25000
6	49692	Curly	3000	Mgr	5	65000	20000
7	34791	Dabarrett	7000	Sales	2	45000	10000
8	84984	Daniels	1000	President	8	150000	100000
9	59937	Dempsey	3000	Sales	3	40000	10000
10	51515	Donovan	3000	Sales	2	30000	5000
11	48338	Fields	4000	Mgr	5	70000	25000
12	91574	Fiklore	1000	Admin	8	35000	---
13	64596	Fine	5000	Mgr	3	75000	25000
14	13729	Green	1000	Mgr	5	90000	25000
15	55957	Hermann	4000	Sales	4	50000	10000
16	31619	Hodgedon	5000	Sales	2	40000	10000
17	1773	Howard	2000	Mgr	3	80000	25000
18	2165	Hugh	1000	Admin	5	30000	---

I was particularly fascinated by MS-DOS — I could spend hours simply exploring the MS-DOS environment. In addition, there were some interesting games available on MS-DOS that I played, including Quake and Doom. For Quake in particular, I spent more time tinkering with MS-DOS than actually playing the game.



First Encounter with Hacking

At the end of 1998, I went to a bookstore with my mother. As usual, after visiting the martial arts section, I made my way to the computer books section. There, I came across a book that immediately caught my curiosity: “Rahasia Pembuatan Virus Komputer” (The Secrets of Computer Virus Creation), published in 1997 and written by two hackers under the pseudonyms Synomadeous and Denny Zip. Intrigued, I purchased the book.

The book was written in Indonesian and covered techniques for creating computer viruses in MS-DOS using 16-bit assembly language on the 8086 architecture. It included several virus source codes — viruses that spread via files and floppy disks, as well as Master Boot Record (MBR) viruses that infected boot sectors. Infecting .COM files was simpler than .EXE files due to their smaller size and straightforward structure.



To compile the assembly source code from the book, I needed a compiler and linker. I downloaded TASM (Turbo Assembler) 2.0 and its linker TLINK (Turbo Linker) 1.0 from the internet. After compiling and linking the code, I released one of the viruses from the book into my school's computer lab. As a result, every student who needed to use the computers for practice was unable to do so due to the damage caused by the virus I had spread.

Eventually, I was called in by a teacher — I was suspected because I was the one most frequently found in the school lab. As a consequence, I was suspended for three days.

Some well-known viruses at that era : ufo virus (created by indonesian virus writer), denzuko virus (created by indonesian virus writer, suspected to live in Bandung), alexander virus, stone virus, etc.

Returning to Being a Normal Student



After the three-day suspension, I learned my lesson and stopped spreading viruses in the school lab. My days in the lab were spent studying WordStar, dBASE III Plus, Lotus 1-2-3, MS-DOS, Microsoft Excel, and Microsoft Word on Windows 98.



Getting into Trouble Again

Before being accepted into a public university and enrolling in an economics program, I spent one year studying Management Information Systems at a polytechnic called AMIK Masa Depan.



At this institution, I studied various new programming languages, including Pascal, Visual Basic, and JavaScript. Of all of them, Pascal was my favorite. Since I did not have a computer at home, I often wrote Pascal programs by hand in a notebook with a pencil, planning to type them up later on the campus computers.



The compiler I used for Pascal was Turbo Pascal version 7.0, which ran within the MS-DOS environment.

```
File Edit Search Run Compile Debug Tools Options Window Help
PRNFLTR.PAS
const
  MaxAttributes = 8;

type
  TPCharArray = arra
  PPCharArray = ^TPC

  PPrinterCodes = ^T
  TPrinterCodes = re
    { Number of pr
  PreambleCount: B
    { Pointer to a
    this printer
  Preamble: PPChar
    { Pointer to a
    changing the
  CodeArray: PPCha
    { Array of indexes into the CodeArray corresponding to attributes
    supported for this printer. }
  Attributes: array[0..MaxAttributes - 1] of Byte;
    { Codes sent at the start of a page. }

75:1
F1 Help | Welcome to Turbo Pascal. Press Enter to close this dialog box
```

```
About
Turbo Pascal
Version 7.0
Copyright (c) 1983,92 by
Borland International, Inc.
OK
```

At AMIK Masa Depan, I got into trouble again. I carelessly spread a Windows computer virus built with Visual Basic. Because I was the one who was most visibly spending all day in the campus computer lab tinkering with machines, the lecturer immediately knew I was responsible. I was called into the faculty room and reprimanded, though a few of the lecturers appeared to be suppressing smiles — perhaps amused to encounter such a computer-obsessed student.

Acceptance into a Public University



After a year at the polytechnic, I sat for the national public university entrance examination and was accepted. I consequently did not continue my studies in Management Information Systems. I was enrolled at Jenderal Soedirman University (UNSOED) in the Department of Development Economics.

My Days as a Script Kiddie

During my university years, I spent countless hours in the library, the campus computer lab, or at internet cafes. Online, I frequented public-access Unix systems (SDF Lonestar and M-Net Arbornet), IRC channels, BBS platforms, and Gopher.

There **were** various security **sites** that I **used to visit** at that time, such as...

<https://web.archive.org/web/20010302030916/http://www.guninski.com/>

phrack.org

<https://web.archive.org/web/20010721220134/packetstormsecurity.com>

<https://web.archive.org/web/20010202072100/http://hackers.com/>

<https://web.archive.org/web/20010224174743/http://www.astalavista.com/>

<https://web.archive.org/web/20010119000200/progenic.com>

<https://web.archive.org/web/20010203133300/http://blacksun.box.sk/>

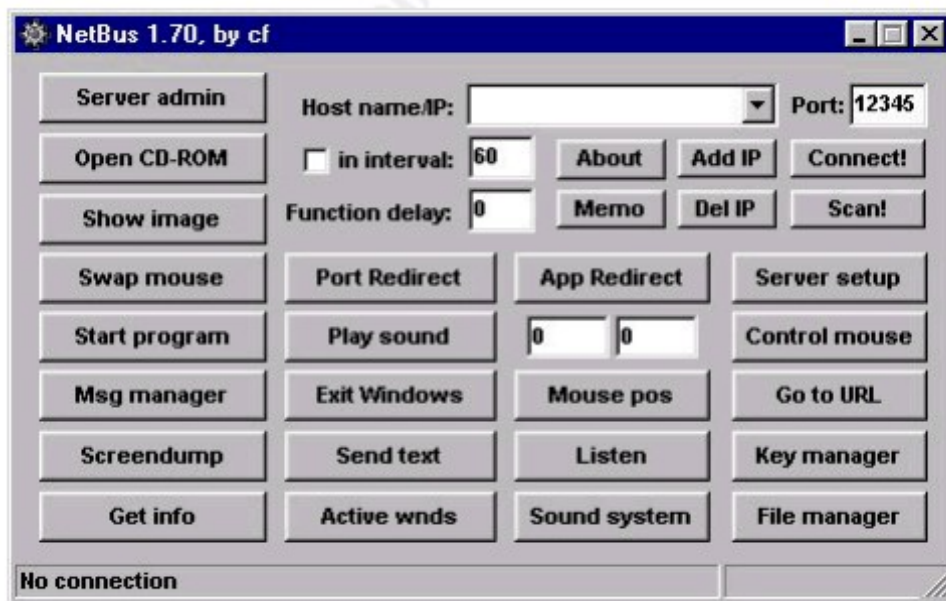
<https://web.archive.org/web/20010202053900/neworder.box.sk>

<https://web.archive.org/web/20010208164128/http://team-teso.net/>

<https://web.archive.org/web/20010209124902/w00w00.org>

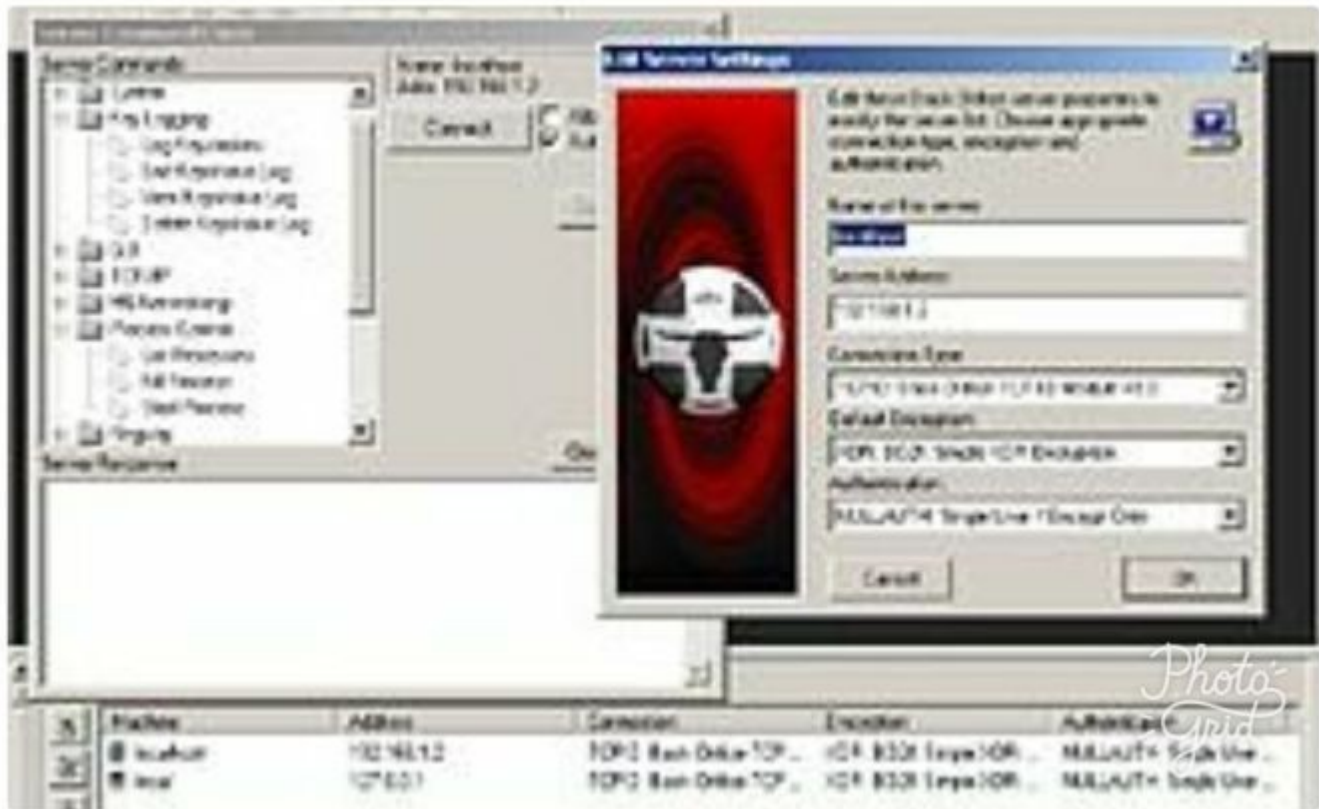
<https://web.archive.org/web/20040708083715/http://thc.org/>

I also engaged in mischievous activities such as downloading trojans from [astalavista.com](http://www.astalavista.com) and installing them on other computers within the local area network.

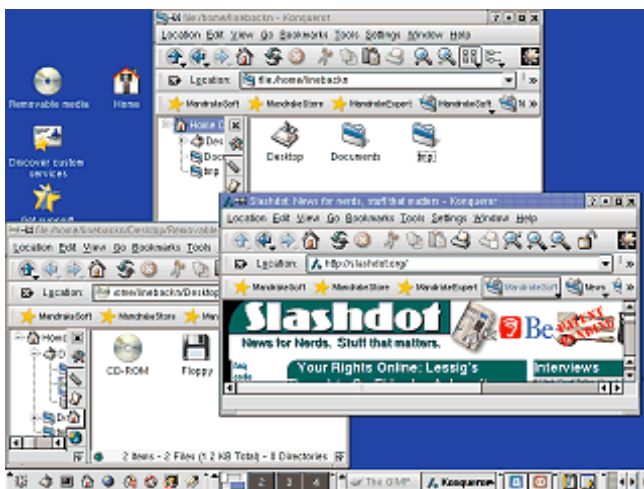


Some well-known trojans of that era included NetBus and Back Orifice by Cult of the Dead Cow. NetBus was notable for disguising its client as a Whack-a-Mole game, so victims had no idea it was a trojan horse. The tool I used most frequently was Pest version 3.1, which was available for download on [astalavista.com](http://www.astalavista.com). Using the trojans I installed, I was able to see what victims were browsing, move their mouse cursor, and send keystrokes to their computers.

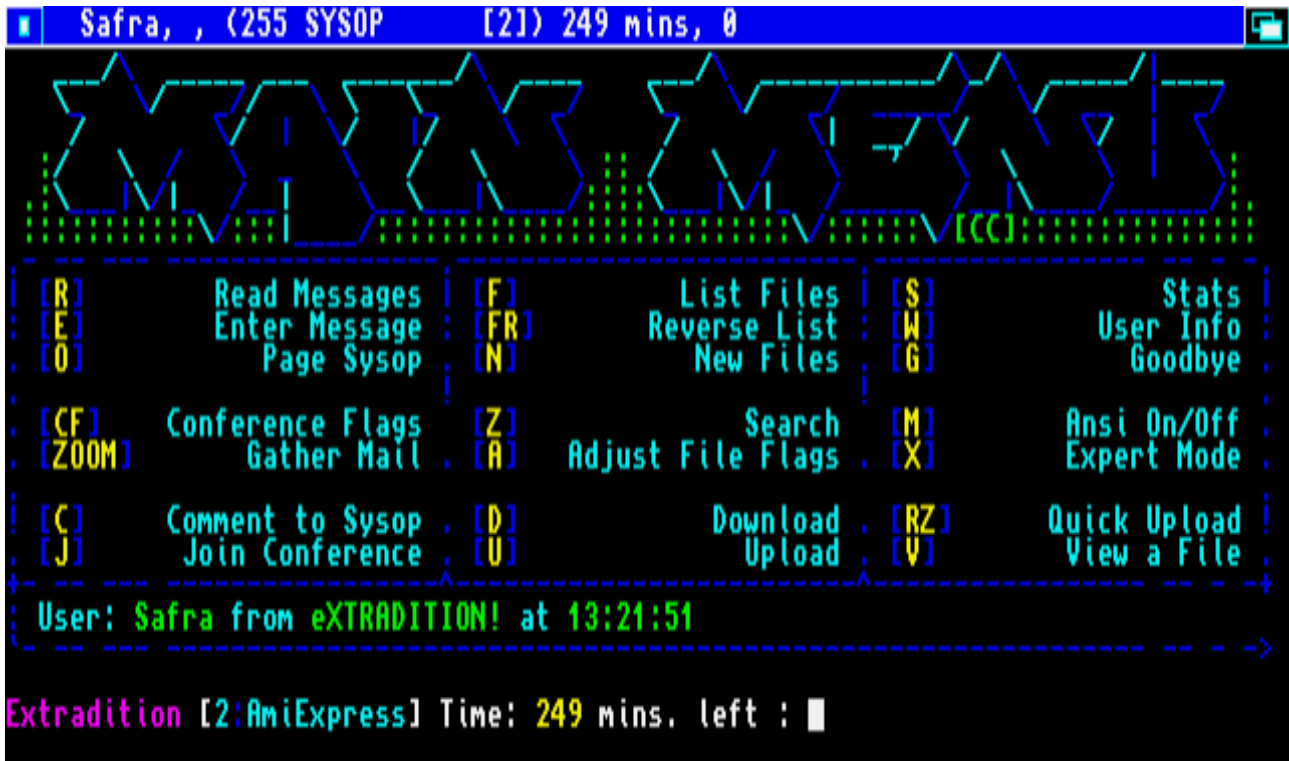
BACK ORIFICE 2000 SHOW SOME CONTROL



Beyond trojans, other tools I used included SuperScan and nmap GUI, JTR (cli), nmap (cli), hydra. For exploits, I used exploits such as the iis webdav exploit, wu-ftpd exploit, iis unicode exploit, etc which I compiled on a campus computer running Mandrake Linux 9.



At the time, BBS and Gopher were rarely accessed by the general public — I continued using them because I was a nerd. BBS, which had previously been accessible via dial-up, had by then largely transitioned to being accessible via Telnet on port 23.



During that period, there was a particularly interesting public-access system running OpenVMS. As of 2026, there is still one public OpenVMS server that can be tried (though it is a new server): <https://encompasserve.org>

Hacking Scene in Indonesia (2001–2004)

I didn't socialize with Indonesian hackers at all, I have been afraid of being ostracized from May 1998 until the end of 2006.



692×291 57.3 KB

I visited the 'Kecoak Elektronik' website around 2001. I found it quite amusing that the site displayed the visitor's IP address, considering that it can be easily implemented using a simple PHP snippet: `<?php echo $_SERVER['REMOTE_ADDR']; ?>`

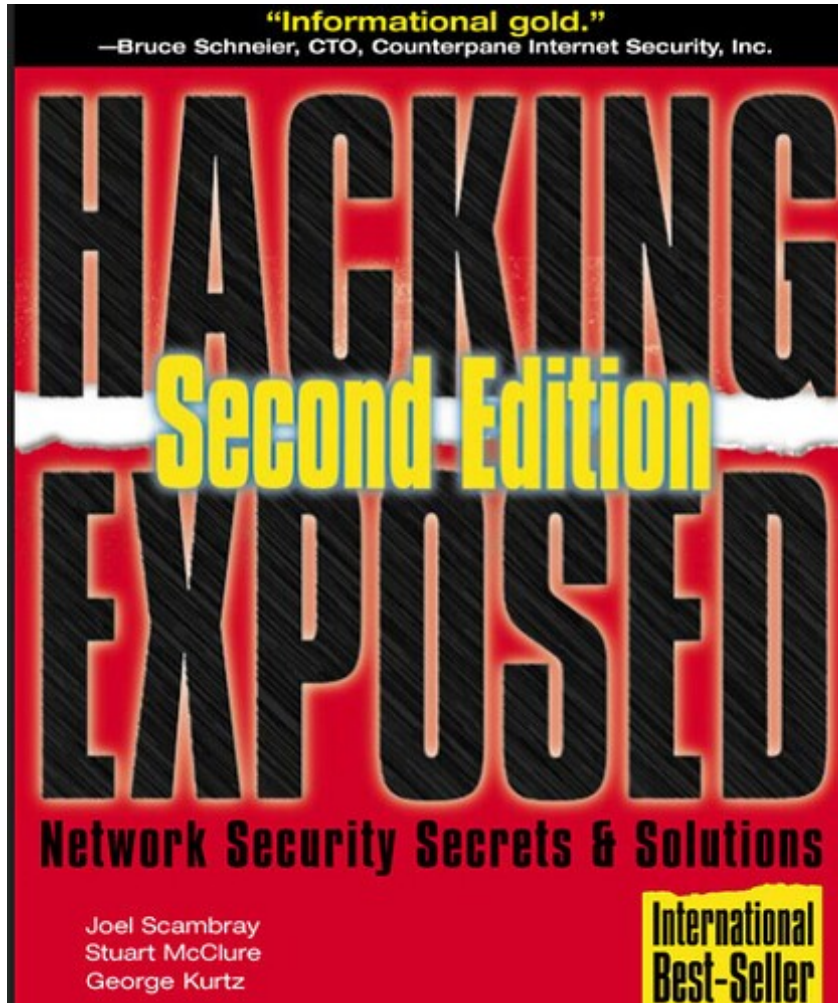
In 2003, I saw some Indonesian hackers founded a new community called echo.or.id

Press enter or click to view image in full size



Books on Hacking

During my time in the university library, I frequently read both economics textbooks and computer books. The book that captivated me most was Hacking Exposed, which covered a wide range of hacking techniques — from network and service exploitation to Unix hacking.



My First Hacker Group



sdf.org

Public Access UNIX System

Non-commercial Internet community

<http://sdf.org>

<gopher://sdf.org>

<telnet://sdf.org>

SDF Lonestar was a very well-known public-access Unix system at the time. Among the people who frequently accessed SDF around 2002–2003 were:

1. smj (sysop) — Stephen Jones, the owner of SDF Lonestar (to my knowledge).
2. karamoon — a network administrator.
3. andiroo — a 13-year-old from the United States who, at that young age, was already capable of breaking into other people's servers.
4. underlan — — a teenage hacker, I still remember his website at that time ! it was :
<https://web.archive.org/web/20021127171742/http://underlan.feckov.org/>
5. evidence — a teenage hacker from Croatia.
6. getch — a teenage hacker from Greece.

In 2003, while I was in the public chat room of the SDF Lonestar public-access Unix system, I witnessed some of my acquaintances beginning to form a hacker group called Solhack. I offered to join, and thus the Solhack teenage hacker group was formed, with its members being the regulars of SDF Lonestar.

<https://web.archive.org/web/20040810013439/http://www.solhack.ath.cx/aboutus.html>

Main	
Home	
About Us	
Submit To Us	
Wargame	
Forum	
Members Only	
Affiliates	
Links	
Wordlist	
Search Engines	
Tutorials	
Network/Security	
Operation Systems	
Encryption	
Programming	
Cracking	
Other	
Source Code	
Exploits	
Disclaimer:	
<p>This site is a portal for all hacker that belive in strong ethics. We do not encourage any criminal activities. Every information on this site is for educational purposes ONLY If you use any program, source code or information in any tutorial on this site to commit illegal actions it is your fault and not ours. This is a place where people that like to learn and to break limits of computer science and belive in freedom of information, speech and data can found their heaven.</p>	
About Us	
Evidence	
Country	: Croatia
Age	: 16
Skills	: c(system & socket programming),c++,perl,shell scripting,php.java script,html,css ,...
Getch	
Country	: Greece
Age	: 16

sol957x616 53.2 KB

web.archive.org/web/20040419145005/http://www.solhack.ath.cx/aboutus.html

.solhack.ath.cx/aboutus.html

Go AUG APR JUN 19 2003 2004 2005

Tools	Skills : c(system&socket programming),c++,perl,html,etc...
Downloads	Foxy
UNIX iso	Country : Netherland
Hacking tools	Age : 18
Various apps	Skills : System administration,c,c++,perl,etc...
Cyber News	lkon
Security News	Country : USA
World news	Age : 18
Sons Of Liberty	Skills : c,c++,php,etc...
	Wisdom
	Country : Indonesia (but Chinese)
	Age : 18
	Skills : :visual basic(data base programming),php&mysql,ASP &access
	c(system&socket programming),c++,pascal,basic.java script,java,graph design,Oracle
	Contact :mywisdom2003x@yahoo.com.sg
	Ncode
	Country : Greece
	Age : 15

image786×456 49.9 KB

Solhack Activities

Among Solhack's activities were the development of computer programs and hacking tools. I was part of an ethical hacker group — though in truth, I also engaged in certain questionable activities independently, without involving other Solhack members, such as rooting servers, attacking IIS servers (typically via IIS Unicode exploits), exploiting CGI vulnerabilities in web applications, and using remote exploits.

<https://web.archive.org/web/20040711082420/http://www.solhack.ath.cx/tools.html>

2004

I got my first pc, I installed microsoft windows xp and mandrake linux 9 at that pc.

At that time, I became addicted to playing Windows games such as **Age of Empires**, **Counter-Strike 1.6**, and other war strategy games. Due to excessive use, my PC eventually burned out in just seven months



image600×342 112 KB

A Hiatus from Hacking

From 2005 to 2007, I stepped away from the hacking scene. In addition to being busy with my studies, I was also occupied with running my own business — a website and software development service called [antonsoft.com](http://www.antonsoft.com).

<https://web.archive.org/web/20050212001057/http://www.antonsoft.com/>

Social Engineering (2006–2007)

Between 2006 and 2007, I carried out a social engineering scheme by creating a fictitious investment website (investasiplus.com). The scheme involved building an attractive website that lured people into investing, with the promise of profitable profit-sharing returns. The result was significant — hundreds of people were successfully deceived into making investments.

https://web.archive.org/web/20060501000000*/investasiplus.com

I accepted payments via banking transfer and e-gold !

Return to Hacking

In 2008, I returned to regularly visiting Indonesian underground forums such as Jasakom. I also began actively writing articles on those forums, covering topics such as DNS amplification attacks, SQL injection, and remote exploits, as well as sharing hacking tools I had developed myself.

I also resumed regular access to the SDF Lonestar public-access system and even set up a Gopher site, accessible via terminal at:

```
gopher gopher://sdf.org/1/users/wisdomc0
```

Around 2009, I co-founded an Indonesian hacking forum called Devilzc0de, along with several other members, including:

1. flyff666 — a 15-year-old with the ability not only to hack servers, but also to infiltrate ISP networks.
2. petimati — serving as the chairman of the forum.
3. chaer — a network administrator.

Devilzc0de remained active until 2015, when it was dissolved due to the members' various professional commitments.

Beyond Indonesian forums, international hacking forums and websites I frequently visited included: milw0rm (exploit publication), hacky0u (security forum), darkc0de (where I often shared tools I had developed), and Packet Storm Security (exploit publications, security articles, and tools).

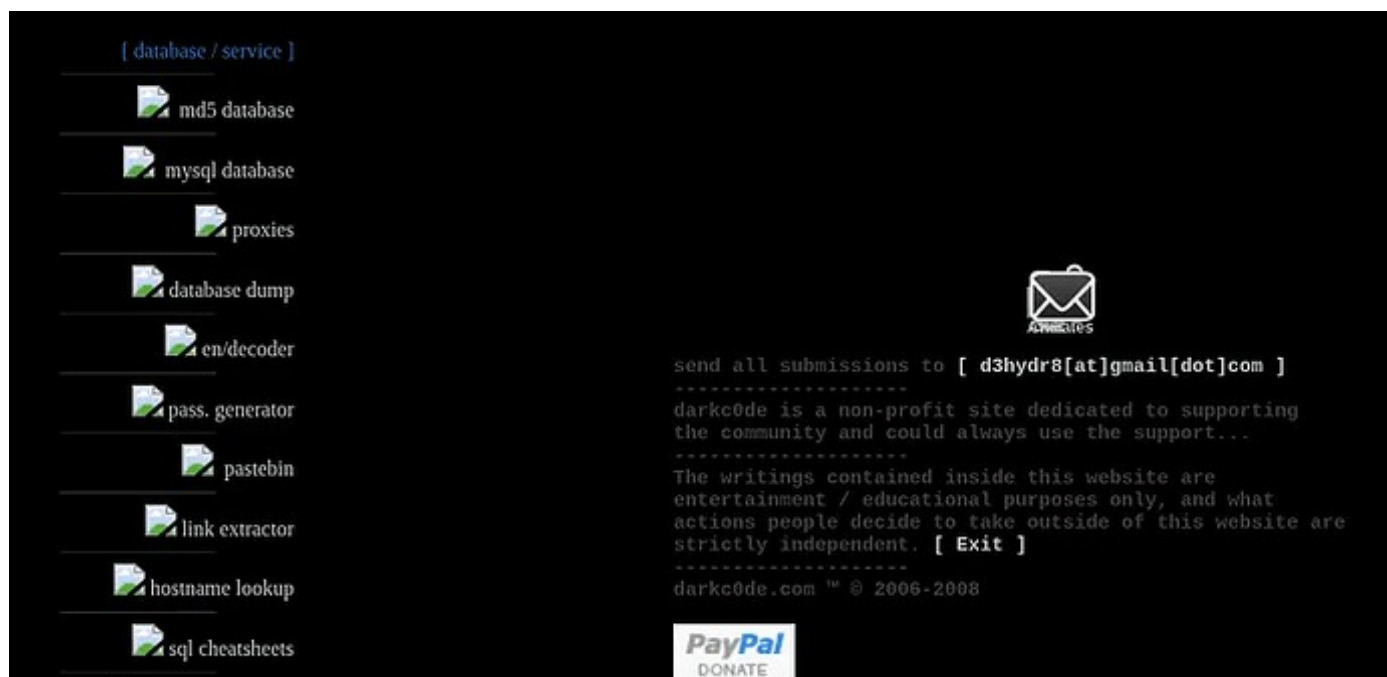


image786×381 74.2 KB

https://web.archive.org/web/2006050100000*/devilz0de.org/forum

Contributions to Packet Storm Security



image786×323 61.9 KB

<https://packetstorm.news/files/author/10292/1>

I began submitting shellcodes, exploits, tools, and other resources to Packet Storm Security starting in 2010, and I came to know the person running the site — a man named Todd, who has always been very kind to me. I sincerely wish him good health and a long life.

Ventures into Robotics



image786×130 34.8 KB

Building on my background in electronics, I began building robots in 2013. I documented my projects on a blog at <https://sw0rdm4n.wordpress.com> , and some of the robots I built can be viewed at <https://www.bluedragonsec.com/var/robotic/>

<https://www.youtube.com/antoniusringlayer>

2013 to 2015

In 2013–2015, I was recruited by a state intelligence agency focused on counterterrorism, during a period of heightened concern over the ISIS threat. My responsibilities included tracking the whereabouts of terrorist suspects and conducting penetration operations against radical Islamic websites.

In 2015, I also built a Wi-Fi hacking robot and demonstrated it during an IT security training session I delivered for BPPT (the Agency for the Assessment and Application of Technology).



image742×453 48.9 KB

The training I conducted at BPPT covered exploitation techniques on Windows — including the fundamentals of stack overflow, Structured Exception Handler (SEH) exploitation, and egg hunters — as well as Linux topics, including remote stack overflow exploitation, bypassing Stack Smashing Protection (SSP) via byte-by-byte brute force, and ASLR bypass using Return-to-libc (ret2libc).

<https://www.youtube.com/watch?v=GSIHgUB-yaA> (this video actually taken in 2015, reposted 6 years ago)

2016



image250×379 22.2 KB

In 2016, I was engaged by the son of a senior police general in Indonesia, with the task of developing Wi-Fi hacking devices and IMSI catchers. Those who are interested in hardware hacking will likely recognize some of the devices I worked with, such as the RTL-SDR, HackRF, and BladeRF.

2017–2019

I developed an open source dns server for linux and freebsd, it's called rldns :

<https://packetstorm.news/search/?q=rldns&a=files>

bluedragonsecurity/ rldns



rldns is an open source lightweight DNS server for linux, netbsd, freebsd, and openbsd. Runs on x86 and x86_64. Latest...

1 Contributor 0 Issues 3 Stars 0 Forks



[GitHub - bluedragonsecurity/rldns: rldns is an open source lightweight DNS server for...](#)

rldns is an open source lightweight DNS server for linux, netbsd, freebsd, and openbsd. Runs on x86 and x86_64. Latest version : rldns-1.4 - released on Feb 2026

I did fids (flight information display system) installations for airports in Indonesia



image600x350 85.7 KB

Failed Startups

In 2020, I was less active in the security field because I was busy with my first startup — a solar panel installation service company called Freenergi. With nothing more than business cards, a home office, and a handful of outsourced staff, I boldly launched the venture. Unfortunately, it failed.

<https://www.youtube.com/@Freenergi>

Undeterred, I attempted another startup — Robotsoft — which produced IoT devices that I designed and built myself.

<https://www.youtube.com/@robotsoft>



image685×398 47.3 KB

Sadly, this venture also failed. I continued attempting additional startups through 2025, but all of them ultimately ended in failure.

It is worth noting that I have been running all of these businesses entirely on my own. Perhaps one day I will find success if I have the right business partner.

Identity Concealment

From 2003 to 2024, I regularly concealed my identity in underground circles, never using my real name. Over the years, I adopted various nicknames, including mranon, ev1lut10n, sw0rdm4n, b4tm4n, wisdom, mywisdom, and d4r3d3v1l. Today, I use my real name — Antonius — for the purpose of advancing my professional career in IT security.

My Secrets to Staying Youthful (Bio Hacking)

I practice **biohacking**. Some of the simple biohacking methods I regularly follow include consuming herbal supplements.

The herbs I frequently consume include:

- **Goji berries**
- **Centella asiatica** (Gotu Kola)
- **Ginseng** (Shen)
- **Fo-ti** (He Shou Wu)
- **Lingzhi mushrooms** (Reishi)

“Actually, there are other biohacking techniques that I practice to make my face look younger, but for certain reasons, I can’t share them.”

And I practice 4 different martial arts : muay thai, tae kwon do, boxing, brazilian jiu-jitsu

2026

There is a notable IT security community in 2026 called <https://0x00sec.org>, which I occasionally visit.

