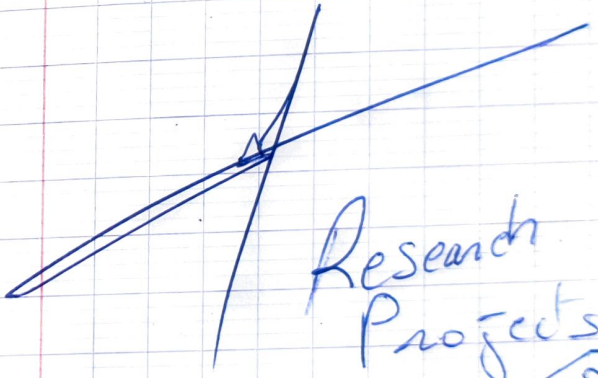
Assessment

December ⟶

2011 – 2012



Research Projects

APPROVED

Kaspr AV 12

ORGANIZE

- Proactive Protection service
- web protection service
- ~~Network~~ Cloud service
- System Monitor service

} connected to ~~DOTPS~~

- Genetic Reparation engine
- Virus Cleaner
- Code Processor

} Virus cleaning Lib

- Advanced Scan Engine
- Advanced ~~System filter~~
- ~~Lib~~ Bitfilter

} CPF Lib

Describe Component

Kaupot AV 12

ORGANIZE

- Proactive Protection service
  - Web protection service
  - ~~Network~~ Cloud service
  - System Monitor service

connected to ~~HTTPS~~

- Genetic Reparation engine
- Virus Cleaner
- Code Processor

Virus cleaning Lib

- Advanced Scan Engine
- Advanced ~~System filter~~ CPF Lib
- ~~File~~ Bitfilter

Describe Components

NIPS

- verify Data Size
- connection ID
- Block Code
- Block object
- Block traffic for IP
- Block As a (page / Script)
- Block Response code
- Block Unwanted port

Packet CAPTURE

- Monitor all packet's
- Alert for unwanted packet's
- Alert for ~~Undefined~~ corrupted packet's

~~PROXY~~

Activation

- Serial, User, Password
- Single Machine INSTALL
- PID
- Install Prove

~~Back~~ VDB

- Manage all connection between KPAV & VDB
- Manage Databases
- Update Databases

Scan Manager

- Manage All scan types
- Manage all Scan Engines
- call scan Engines
- interact with GUI of KPAV Scan

Scan Engines

- ASCII Scanner (STRING Scanner)
- PE Type scanner
- Hash scanner
- ~~Hard~~ Archive Scanner
- No Scanner

File format

- check file format with specific scanner
- Verify VDB file format
- Manage Formats

- Proactive
  - ↳ Monitor all files in specific zone
  - ↳ Protection level
  - ↳ Scan any watched file
- Web protection
  - ↳ Monitor all HTTP Traffic
  - ↳ filter all Input data
  - ↳ Include NIPS
- Speech Recognize all command
  - → Recognize Synthesis.

Todo

+ Control Center Html ✓
+ Create a server ✓
+ add Hosts to Virtual Host list ✓
+ ~~Kav~~ Installation provide
+ Single Machine Install
+ System Rescue Component
  - → Detect Last Installed files
  - → Detect Last Reg
  - →

Remove checked list
Remove generate list
use disposer in web check Points

{ Kavprot Proactive service
  Kavprot Network Protection service.

Projet **Next version**

IPDTP V2

- + ~~AUGS~~ (~~Automatic Upl Generator Server~~)
- + ~~SNS~~
- + ~~Send Server SNS Request~~
- + Send IPDTP packets via internet
- + IPDTP Firewall
- + IPDTP Port
- + IPDTP Firewall plugin
- + To prevent Decryption
  - Register { Upl / Password / Server Name

- + ASC Tunel
  - → SECURE Method
  - → REGISTER Method

Final Kavprot AV 2012

STEPS

- → Install Prove (All Informations about PC)
- → Settings (Start IPDTP)
- → CPF
- → Filter data
- → get Entry point Code (GHE)
- → [illegible] Kavprot IPDTP Server
- → Kavprot [illegible] Detect Authenticode
- → Kavprot Gridwall (IPDTP wall)
- → Kavprot VFirewall (Network Protection)
- → IPDTP [illegible] Scanner
- → Start Gridwall (Settings)
- → Start VFirewall (Settings)
- → Online Activation Blocker
- HS Mode { Text scanner → Detect if file size is > (1024 x 1024)
  - Scan file Normal | ELSE (HS)

- → Kavprot Virtual Firewall Filter interface
- → organize (KPAVE) (Protection) (VDB) classes
- → Detect the scanner that uses CPU
- → High sense (Scanner settings)
- → try FTS 3 { SQLite

VFirewall Blocking property

if (DIP = localIP)

SIP	SP	DIP	DP
0	0	0	0
0	Any	0	0
Any	0	0	0
Any	Any	0	0
Any	Any	0	Any
else			
0	0	0	0
0	0	0	Any
0	0	Any	0
0	0	Any	Any
0	Any	Any	Any

Block Incoming

SIP	DIP	SP	DP
0	0	0	0
0	0	0	Any
0	0	Any	Any
Any	0	Any	Any
Any	0	0	Any
Any	0	0	0

SQ Lite Test

	FTS 3		Normal (Indexed)	
	1	2	1	2
Seled exist	x3 fast	x9 fast	x2 fast	x1 fast
Seled not exist	x1 fast	x5 fast	x2 fast	x5 fast
Insert	equal	equal	equal	equal
Reader	x3 fast	x4 fast	x2 fast	x3 fast
Result	25/8		11/8	
	High Score		High Score	

Upgraded from Indexed VDB → FTS3 VDB

→ Change all VDB Methods ✓
by FTS3 → optimize CDLL usage ✓
by FTS3 → optimize memory usage ✓

KProxy ✓

- → Fix all errors ✓
- → optimize code ✓
- → Replace all Responses ✓
- → Replace all Codes ✓
- → Fix log path ✓
- → Rename Classes ✓
- → Remove prefs tg file KProxy.klist
- → Remake ReG Reader ✓

Integrate KProxy lib in WebPost lib

→ Remove Filter interfaces ✓
→ Remove VFirewall ✓
→ Allow DB Share ✓
→ Password Access ✓

→ Local Copy of Dotnet Bar and ✓
→ Extract Archive Percentage ✓
→ Scan Form Notifier ✓
~~→ Web Protection~~
≃ Kavprot Command line Scanner ✓
→ Fast initializer ✓
→ Kavprot LIE.exe → Kavprot.exe ✓
→ Kavprot Memory optimization ✓
→ setting Anti-Spam ✓
→ optimize the code and performance ✓
→ organize classes ✓
→ Kavprot speech optimize ✓
→ change Splash screen UI ✓
→ User Communication (GUI upgrade) to be ✓
→ Kavprot Log profile on FTP server ✓
→ Kavpot IPOTP Service ✓
change → Local Hostpage . 127.0.0.1:8778 ✓

→ change Icon ✓
→ Filter post Method ✓
→ Test for 1 Last day 14 hours of Protection
→ Release
→ Test 5 days or 30 days
→ Publish

Test Full scan

Memory before FS 308 MB

after FS

→ Check if ASCII Scanner works

Verify → Trojan Downloader.Bagle.ntk
Verified by
ASCII Scanner
and Hash Scanner

C:/AUTOEXEC.bat
C:/Windows/control.ini

FIXED FalsePositif

Alert By HDB

Code optimization

→ prevent IOException
→ prevent exception
→ UnAuthorized Access Exception
→ Stream reads without filestream
ASCIIScan

Methods to optimize
→ Dump Hex (ASCII Scanner)
Proactive on changed
→
→ Main Forms.Init
ShowModal panel
if null → Init, Load
else nothing
→ Remove Save session
→ organize Log
ExLog
AppLog

→ Rename protection Log →
→ Settings fast boot Exceptions
→ Setting Save Session

websites

AVL : Kavprot- ~~Latest~~ Virus signatures.

AVL : Issues

Requested pages by kavprot

Kavprot final Devsteps

→ Post Virus Report Service informations

→ ~~Kavprot license Library~~

→ ~~Kavprot Security Assembly~~

→ Change Activation Method

For performance

→ attack Memory ↗ ports and optimize them

→ Scanners

→ File Reader (I/O)

→ lists

Kaspot ASBHT
Anssleusoft Basic Hard Test

- Protection ✓ 10/10
  - Start ✓ 10
  - Kill ✓
  - StartProt ✓
  - Cloud ✓
- Engine 10/10
  - Scan ✓
  - Scan HS ✓
  - Scan F ✓
- Scanners RTP ✓ 10/10
  - ASCII ✓
  - PE ✓
  - Hash ✓
  - No ✓
  - ARCH ✓
- FileFormat 10
- ScanEngine 10
- URPS 10 ✓
- Proactive 10 ✓
- WebSD 10 ✓
- Safe browse 10 10
- POST 10 ✓

NIRS	9,8 ✓
ANtiSpam	10 ✓
Local Host	10 ✓
Speach	10 ✓
Passgen	10 ✓
Backup	10 ✓
Smart backup	10 ✓
Quarantine	10 ✓
Remove	8 ✓
detection	10 ✓
speed	9 ✓
Alert	10 ✓
GUI	10 ✓
VDB	10 ✓
Network (UFWR)	10 ✓
Drive Monitor	10 ✓
Activation	10 ✓
log	10 ✓
Anticrash	10 ✓

286,8
290

Kaspot ASPT
Anssleusoft Preaformance Test

boot Speed	10/10 ✓
Speed	10 ✓
CPU	10 ✓
Memory	9 ✓
Disk usage	9 ✓
SELECTION Speed	10 ✓
Insertion Speed	10 ✓
Scan speed	10 ✓
ASCII Speed	10 ✓
PE. speed	10 ✓
Hash speed	10 ✓
ARCH speed	10 ✓
No speed	10 ✓
GUI Communication speed	10 ✓
GUI	10 ✓
No Lags	10 ✓

158
160

Kavprot ASPQT
Anslasoft Product Quality Test

Performance 158/160
GUI 100 ~~280~~/100
Basic quality 286/290

Protection 498/500
Detection Ratio 1500/1500
Cloud 100/100
Report 100/100
VDBT 100/100
Support 100/100
Easy to use 100/100

99,62

$$\frac{1992,5}{2000}$$

Test Result

$$\frac{1992,5}{2000} = \frac{99,625}{100}$$

99,62

0,62

99/100

Fireweb Navigator 7.0

* Metroshell theme
* Gecko 8
* Report Form exception
* optimize code (StreamReader, Bender instances)
* Treco international
* Remove optimize (Empty working set
* xulRunner 8.0
* Safe browsing VDB change to VDB Kavprot
* web smart Detection detect title
*

$$\sum_{i=1}^{4} (x)^i = x^1 + x^2 + 2^3 + 2^4 = 16 + 8 + 4 + 2 = 30$$

$P(x) = 1/30$ $\quad y = 4$ $\quad y_{max}$ $\quad y_{min} = 1$

$x^1 + x^2 + x^3 + x^4 = 30$

$30 - x^4 + x^3 - x^2 - x^1 = 0$

$P(x) : 4$

$30 - 2^4 - 2^3 - 2^2 - 2^1 = 30 - 16 - 8 - 4 - 2$

Kaspersky Key

$$\frac{1}{2176782336 \times 10^{12}}$$

60 element $\quad y = 12$

$x = 60$

$P(x) = (x)^y = 60^{12} = 2176782336 \times 10^{12}$

ERRORS

Alert: update prog : Scan completed → Header

Quick scan : Not win32 folder → Real time life

Publication:

Kaspersky ✓

Kaspersky-FR ✓

Firefox Navigator 7. ✓

Soul of the prince ✓

DS2011 ✓

IPDTP 1.0 ✓

ASN.1 Editor ✓

91 4% 46 11

IOADD7

2010

$1^1 + 1^2 + 1^3 - - = 10^{?}$ 1^{10} Y

Si $x = 1$ et $y_{min} = 1$

$P(x) = y_{max}$

nombre ...

$\sum_{i=1}^{y} (x)^i$

Kaspersk : $1/(60)^{12}$	Telecom $1/(10)^7$
Tunisiana : $1/10^7$	

exemple : $x = 1$ $y = 4$

$1^1 + 1^2 + 1^3 + 1^4 = 4$

x, y et z sont trois entiers naturelle

$y = y_{Max}$ $z = y_{min}$

x = nombre élément

Par exemple pour représenté une image numér... en couleur réel on a une palette composé d' 2^{24} couleur sur 3 octets

App

$x = 2$ $\overbrace{(0,1)}^{2}$ / $y_{Max} = 24$ $y_{min} = 24$

$\sum_{i=2}^{y} (x)^i = \sum_{i=24}^{24} (x)^i = x^{24} = 2^{24}$

Si $x = 0$ impar

Si $y = 0$ impar

Si $x = n$ $y = n$

$(x)^y$

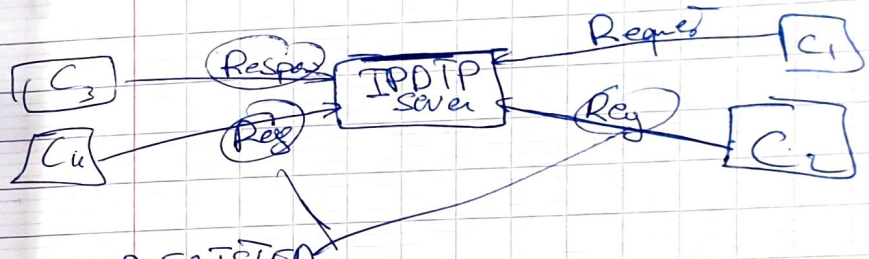
Si $x = n$ $y = n$ $z = n$ $y \neq z$

$$\sum_{z=2}^{y} (x)!$$

Si $x = n$ $y = n$ $z = n$ impar

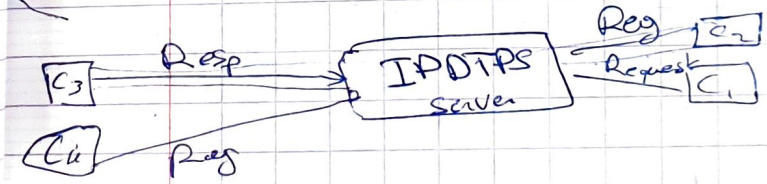
IPDTPS

IPDTP



REGISTER
UPL / Servername

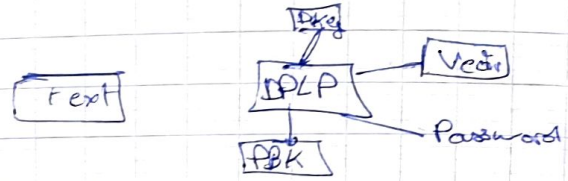
Request / Response = text plain

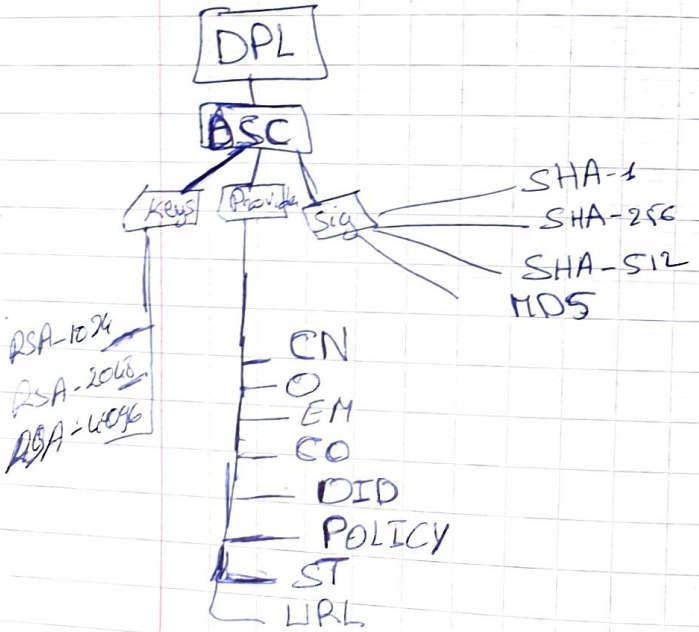


DPL 512
DPL 1024
DPL 2048

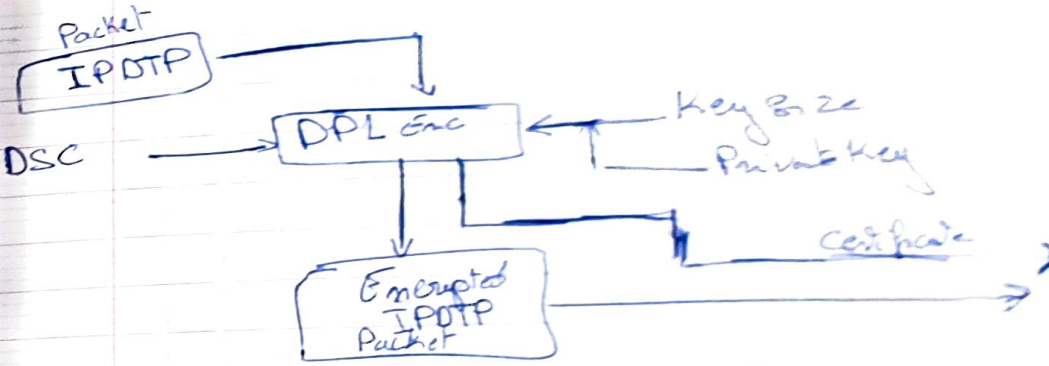
DPL → Data protection layer

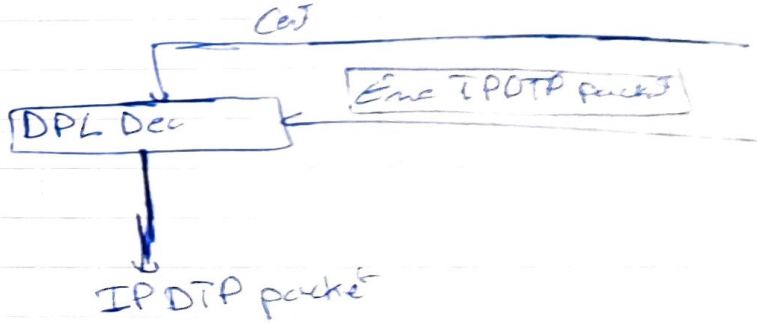
Encryption Algorithm





Encryption / Decryption





IPDTP Tunel

@

x et y deux entiers successif x > y

$x^2 = y^2 + x + y$

App

x = 3 y = 2

$3^2 = 2^2 + 3 + 2 = 4 + 5 = 9$

$3^2 = 9$

x = 4 y = 3

$4^2 = 3^2 + 4 + 3 = 9 + 7 = 16$

$4^2 = 16$

PVK = P(x) * e

P(x) / x = 36

y = KeySize

y = 1024 ⇒ $(36)^{1024}$

PVK = e + (p x q)

x2 KeySize

e = P(x) - pq

d = decoder

p = provider

q = Key producer

ASY = 5

provider / Sy = 4

C = 3

decoder = indéfini

PBK

= PVK x (e x q)

KeySize = 2

App x = 10 y = 2

e = 10 / d = 97 / p = 5 / q = 5

PVK = 100 + $(5 \times 97)^5$ =

Anssleuapt System

Why I will create it?

- Security
  - to detect viruses
  - to secure machine
  - to exploit vulnerability
  - to Hack
  - to encrypt/decrypt
  - to Hash
  - to check a cloud
  - to get security informations
  - to monitor (System, web, Network ...)
- IDE
  - to compile AL, ASPL
  - to edit AL, ASPL
  - to Debug
- Business
  - to manage business
  - to get client informations.
  - ~~get fingers~~
- Cybercrime
  - to identify criminal via fingerprint
  - to get traces of criminal.

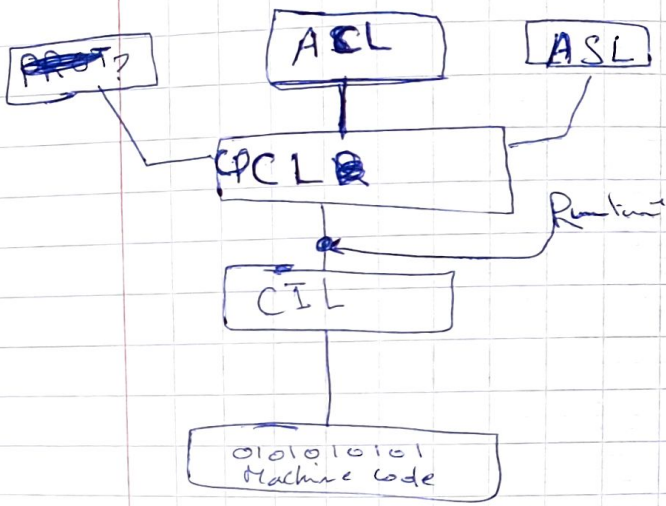
- Web
  - Web browser (IE, Gecko 5)
  - chat TCP
  - send mail
  - ~~x~~
- Tools + (languages)
  - speech Recognizer
  - speech Synthesizer and Studio
  - Speech IDSys (Speech Language)
  - Security Language (Protection Language)
  - log in DB
  - XDF editor
  - IPDTP client
  - Software cache.
  - cyber monitor
  - C# Compiler

to be continued
Inchallah

Developper studio 2011

- Pascal editor (CPL)
- ~~Assglen~~ Assglen Language editor (CPL)
- C#, VB.Net, JS, HTML, PHP, Batch, POO, editor
- speech recognizer
- Compiler interface
- settings-manager
- project parser.
- Intellisense
- ALR (R, C, E)
- ACPE (R, C, E)
- RLL (R, C, E)
- Robot agent
- ~~xxx~~.

Common Precompiled executable Structure



CPCL : common Precompiled language

CPCL Instruction, Program

Program
- PROGRAM
- START
- code
- END

instruction
- INS: (EP) ($)
- code
- EINS;

code
- Bool
- STRING
- CHAR
- INT16
- INT32
- LONG
- VAR
- STRING[x]
- Readline(), Writeline();
- Read(), Write();
- Readkey(), Title();
- Declare lb
- goto
- WHILE
- Power
- PI
- SQRT
- Clear()

example of ASPL x70

ASPL x70

```
10 CLS
20 ekteb " AST"
30 ekteb " Go to the bed"
```

CPL

```
PROGRAM
START
INS : EP
 CLEAR;
 WRITE " AST";
 WRITE "Go to the bed";
EINS
END
```

Example AL

```
function main ()
{
  int a = 5;
  int b = 6;
  int c = b + a;
  print(" Result is ", c);
}
```

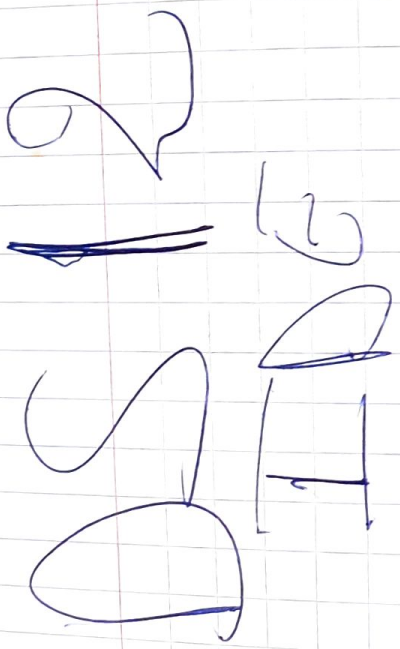
```
PROGRAM
START
INS : EP
 INT32 A IS 5;
 INT32 B IS 6;
 INT32 C IS A+B;
 WRITE " Result is" FORMAT(?) => C
EINS
END.
```

Dev 12 editions

- ~~Pascal edition~~ => Professional = C#, VB.Net
- A2 edition => ~~Ultimate~~ Ultimate
- Starter edition => = scripting, Webpage ...
- Basic edition = ASPL
- express edition = Pascal

Telephone

$C_{19}H_{28}O_2$



DS 12 IDE Main components

Pascal ~~IDE~~

~~C# IDE~~ as plugin
~~VB.Net IDE~~ as plugin
Pascal IDE as plugin
~~AL IDE~~ as plugin
} Plugin Manager

Speech Recognizer
Speech Synthesizer
Robot
} Speech communicator

Pascal compiler ⟶ FPC
compiler plugin
~~Compiler~~
} Compiling Module

Code Security Verification
Code Signature
Code trust Mark
} Pre-compilation Module

Code Hight lighting
Syntax coloring
Text editor
} editor Module

DSS } DSS Module

DSSlib

Project Manager

Command Manager

~ Algorithm Analysis

Code Analysis Manager

[redacted]

[redacted]

[redacted]

[redacted]

DS Pascal editor

Speech SPR, SPS ✓

Console ✓

Messages list ✓

GUI ✓ option menu about menu

- Ressource redor, editor ✓
- Pascal editor ✓
- Pascal compiler ✓
- ~~Solution creator, opener, saver~~
- Pascal assembler ✓

Intellisense cases

ci string No Intellisense

in declaration : only keywords

in

Developer Studio

2013

Project Duration

60 → 90 days

Objectif

Assisten language IDE

C# IDE

JAVA IDE

Pascal IDE

Script IDE

Web IDE

AL Compiler

IL: ASM / DISM

AL ASM / AL DISM

AL Runtime

Flydows Versions

BE:
- Business softwares
- web

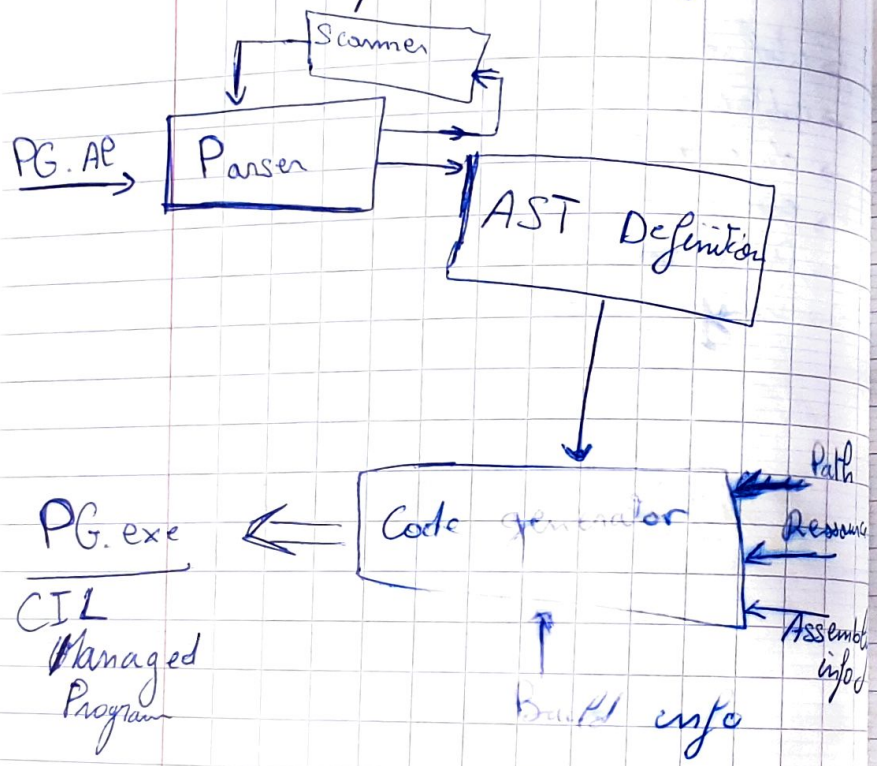
EE
- IDE's
- Compilers
- Entertainment

FE
- Entertainment
- games
- web
- editors
- softwares

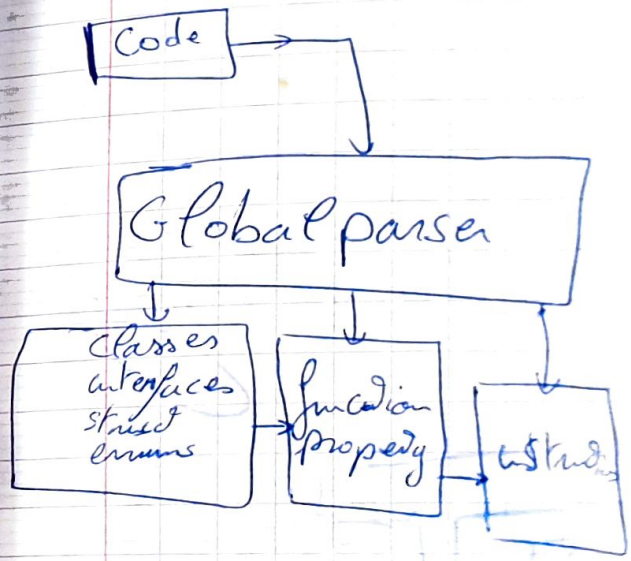
DS12 PBS

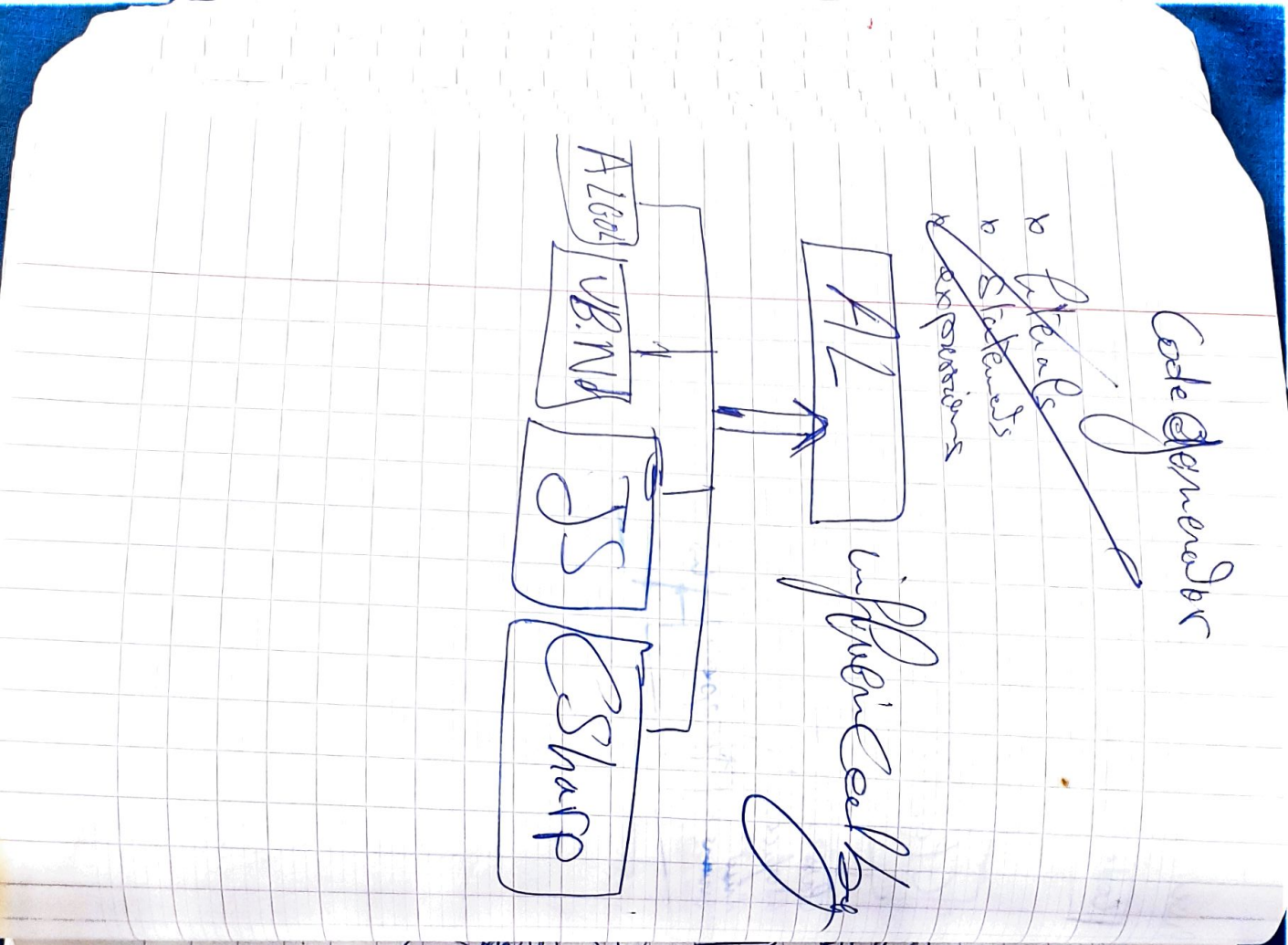
- → Intellisense Add drawed
- → update intellisense file
- → change NS, classes, keywords icons
- → ERROR Report in editor
- → Pascal Debugger
- → Trendy pascal

Arsslen language



Parser





C#sharp 3.0 → AL 2.0

C# Keyword	AL	C#	AL	C#	AL
EOF		default		implicit	
NONE					
ERROR	~~ERROR~~	delegate		in	
FIRST_Keyword		do		Int	integer
ABSTRACT	inheritable	double	~~real~~	interface	
AS		else		internal	friend (inside)
ADD		enum	~~Enumeration~~	is	
BASE	Mybase	event		lock	Secure
BOOL	boolean	explicit	~~Exact~~	long	
Byte		extern	outside	Namespace	Program
~~break~~	~~regex~~	false		New	
Case	State	finally		Null	~~Nothing~~
Catch		fixed		object	Object
Char		float	~~Floating~~ Float	operator	
Checked		for		out	
Class		foreach	for each	override	
Const	Constant	GOTO	goto	params	parameter
Continue	persist	If		private	~~private~~
decimal					

CS	Al	CS	Al	CS	Al	CS	Al
protected		this	myself				
public		throw		while		descending	
readonly		True		ARGLIST		into	
ref		try		PARTIAL	Shared	interm	
return	Backwit	typeof		ARROW		get	get-
remove		UINT	UInte~~ger~~ unsigned int	from		set	Out
sbyte		ULong	ULong~~int~~	from_first		STAR	
sealed	final ~~Unchangeable~~	unchecked		join		~~DIV~~	
short	Short~~int~~	unsafe		on		break	exit
sizeof		UShort	UShort~~int~~	equals			
stackalloc	S	Using	Include	select			
static		virtual	Virt	group			
string		void	Sub	by			
struct		volatile		let			
switch				order by			

A[illegible] language arithmetic operators table and Logical

Operator	Name	~~des~~ objectif	Target ASM
+	unary Plus	add element to another element	x ADD y
-	unary negation	substract element from element	x SUB y
!	Logical Not	give the inversion of a bool value	
~	Ones complement		
++	increment	increment an object	INC x,
--	Decrement	decrement an object	DEC x
*	Multiply	multiply two given elements	x MUL y
/	Division	dibide element by element	x DIV y
%	Modulus	return the rest of division	x MOD y
&	AND logical	returns the logical and result	x AND y
|	bitwise or	return the or of 2 elements	x OR y
^	bitwise XOR	return the exclusive of 2 elements	x XOR y
<<	left shift	—	—
>>	right shift	—	

AL Language Design

Primary design

final design

Developer Studio 2013
Professional edition:

⇒ Editor
→ Intellisense
→ Syntax coloration
⇒ Project mgt
Solution explorer
→ reference explorer
→ compiler
→ Syntax checker
→ * generation manager

DS 12 Project

GUI

DeVSTD
- Components Manager (Windows form)
- Reference Manager (framework Mgr)
- Source Code editor
- Code Parser form
- start page
- about form
- Report
- splash screen
- Solution explorer
- error & Viewer
- Debug window
- object explorer
- Code provider Manager
- Addin Manager
- Add-in

DS Project component .DSP

- Sources
- Assembly info
- Includes
- output.

.al
.alnf
.alref
.alout

Project Content

ASA Projet
IAC Projet

Objective:
* protect computer using cloud
* protect user using proxy
* detect intrusions and send Reports to server
* Block Unwanted files (Remove, delete, encrypt)
* Unblock files (decrypt, Restore)
* Smart online backup
* First line defense With windefender
* User activity monitor (privacy protected)
*

30 days
30 days
45 days
60 days
Management

ASFP
Assistensoft future projects

Developer studio 3.0 Professionnal Edition
- Assistent Language Compiler
- Assistent IL Runtime
- Assistensoft .Net framework 2.0
- Add-in Manager (interfaces)
- ASDN
- Anti-Crash 2.0

Assistensoft Speech Technology 2.0
- Speech acognition
- Speech Synthesis
- Speech IDE
- Speech Interface (GUI)
- speech updates

Assistensoft Firewall Navigator 9.0
- Anti-phishing (expert) + link scanner
- embeded settings, User enterface
- XUrunner (9.0) or (10.0)
- TAC, His, Link, in db

Kaspot Smart Security 2.0
- Antivirus
- Firewall - Anti-phishing - Antispam - IDS
- Cloud
- HIPS
- Updates - Addons
- Valnerability scanner - .... To be added

M-lite Media player 2.0
- Recorder
- player
- Visualisations

XDF Reader + Writer
-

Arssleasoft websites

Home
↳ Html

ASDN
↳ Mediawiki

Forum
↳ phpbb

ASN
↳

~~Blog~~

NDS

Kaspersky Smart Security 2.0

GF
- password protection
- Game Mode
- Alert controller
- Updates

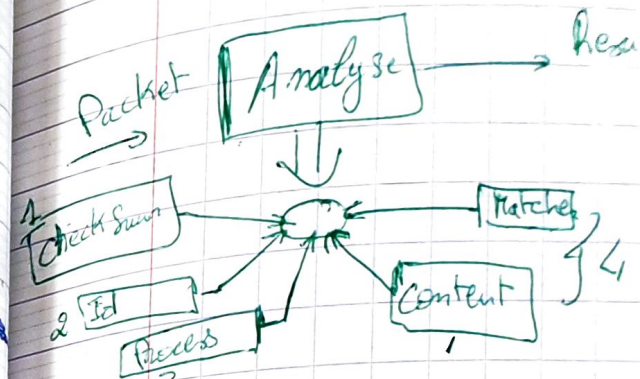
AVF
- Monitoring sensitivity
  - Low :
  - Normal : emails I/O, Web, INS/Msg, files
  - High : web, executable files.
- AVsense
- exclusion

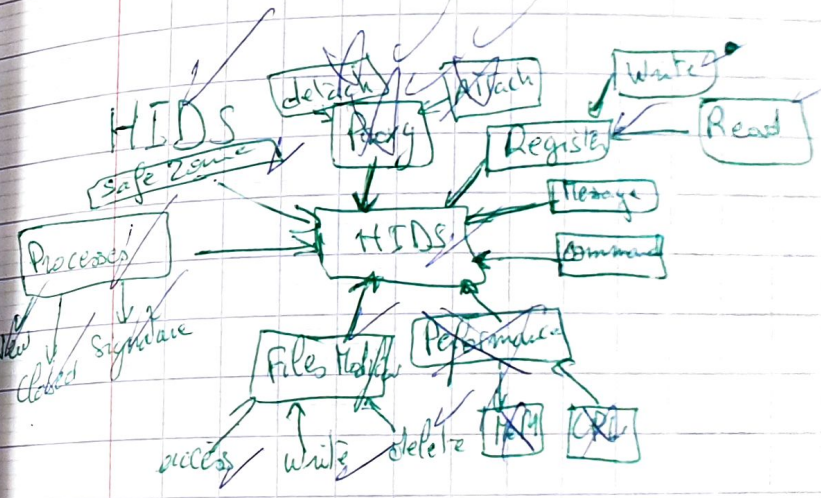
ADSF
- Anti-Vulnerabilities
- Anti-spam
- Quarantine
- Parental control

Web
- Proxy
- Safe browsing
- Firewall

- Event log
- Cloud
- AVDBG
- Add-in

NIDS





⇒ Verify process on execution
→ Verify integrity of informations
→

SDV
or CEV

System Destruction Virus

1 → get all information (send it to server)
get all Texts files
2 → AV Rules
3 → register proxy, run registry
4 → get System security state
5 → decide
destroy

listen
listen to all requests

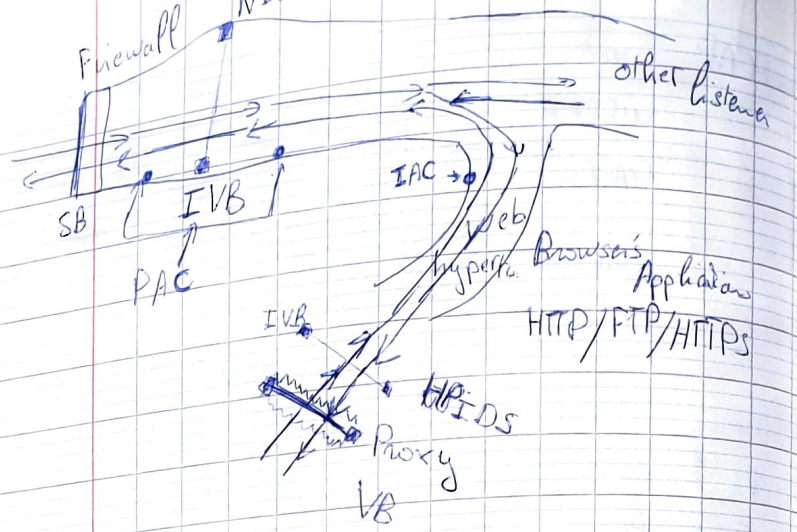
NIDS

WinPCAP
WRAPER
PCAP.NET
N.I.D.S
Result
Alert
Action
check
Analyze
pattern
rules

Firewall

Bad Port
Bad Packet
Safe Packet
Untrusted program
Trusted program
1STD
2SD
first line defense
Second line defense

Honeypot network protection

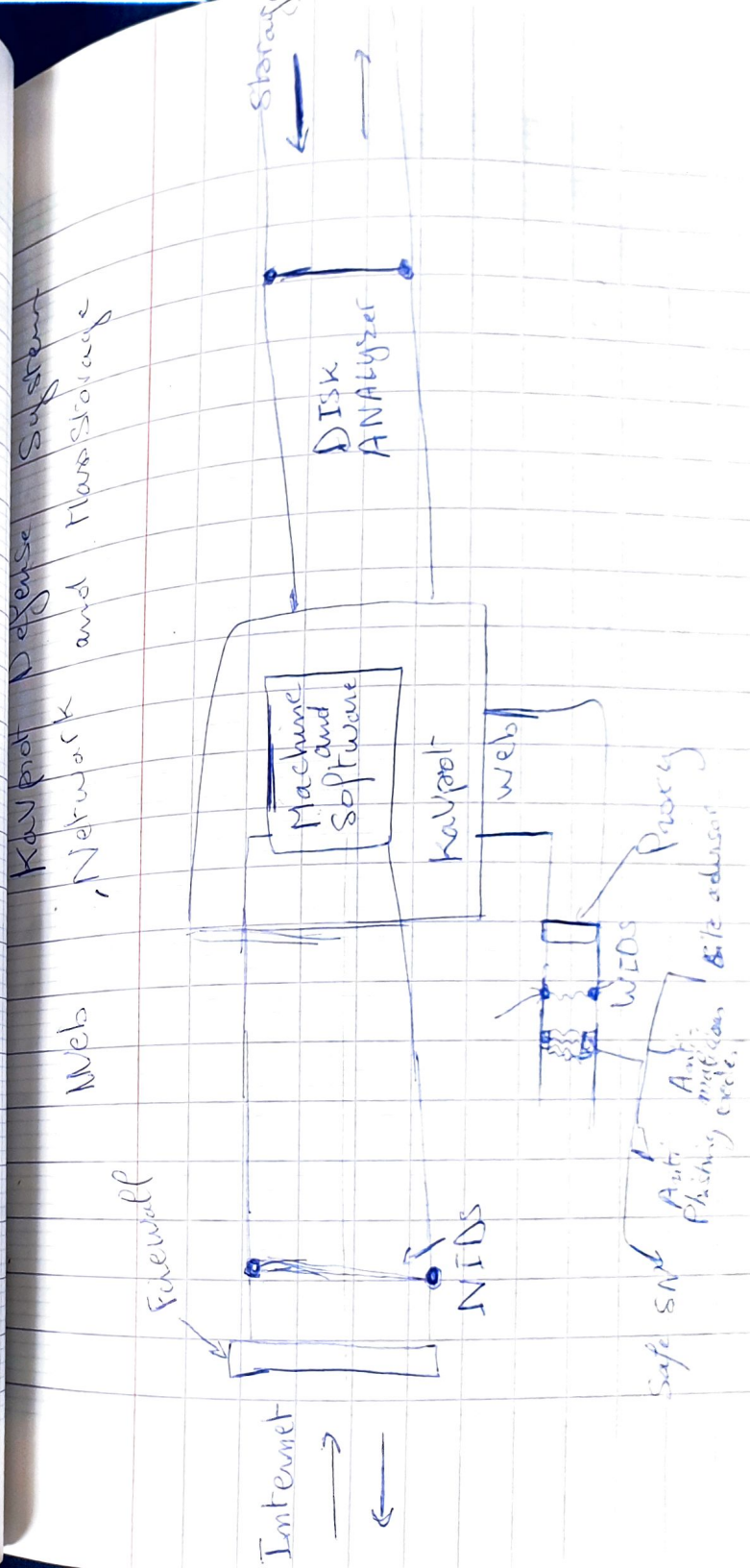


IVB: Invisible Barrier

SB: Strong Barrier

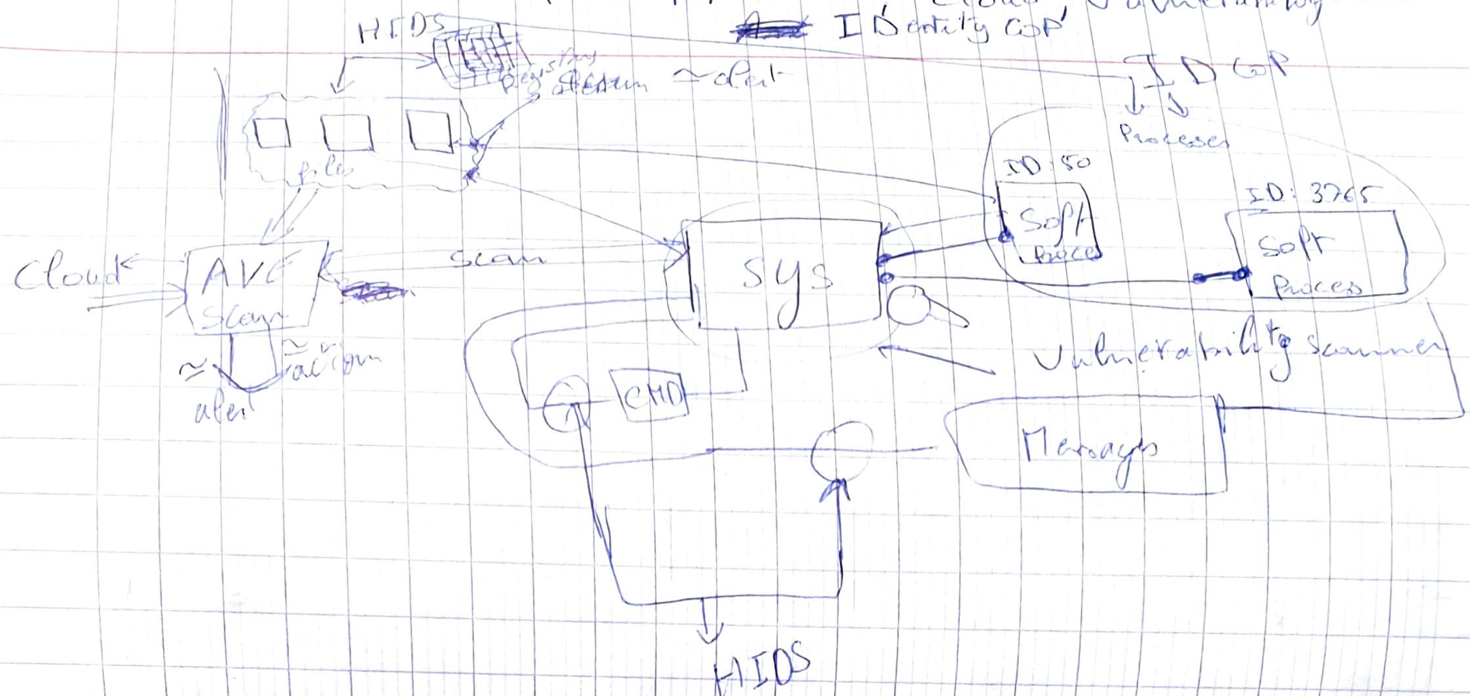
VB: Visible Barrier

A:



Kavpot Defense system

HIDS, Antivirus, Cloud, Vulnerability and Identity COP



Kavpot Defense System Technical Specification

- ~~Sys Event~~ ⇒ Events
- File modified: Scanned with HIDS, AVE, Cloud
- Process started: Scanned with HIDS, AVE, Cloud
- Process stopped: Nothing
- Messaging: Scanned with HIDS
- Registry Access: Scanned with HIDS
- Command exec: Alert By HIDS
- System Modification (time, calendar): Scanned with HIDS & VLS
- Packet IN: Verified by Firewall and NIDS
- Packet Out: Verified by Firewall and NIDS
- Hypervisor: Web protection system verification (6 layers)
- Connected: firewall state
- Process Out: Verified by IDCOP
- Process: Verified by IDCOP
- Binary file: Verified by Trust-Program System (TPS)
- KPAV: Protected by Kavpot Protection Agent (KPA)

Dev: Tools for [illegible]

Nessus : Vulnerability scanning

Nmap : scan port

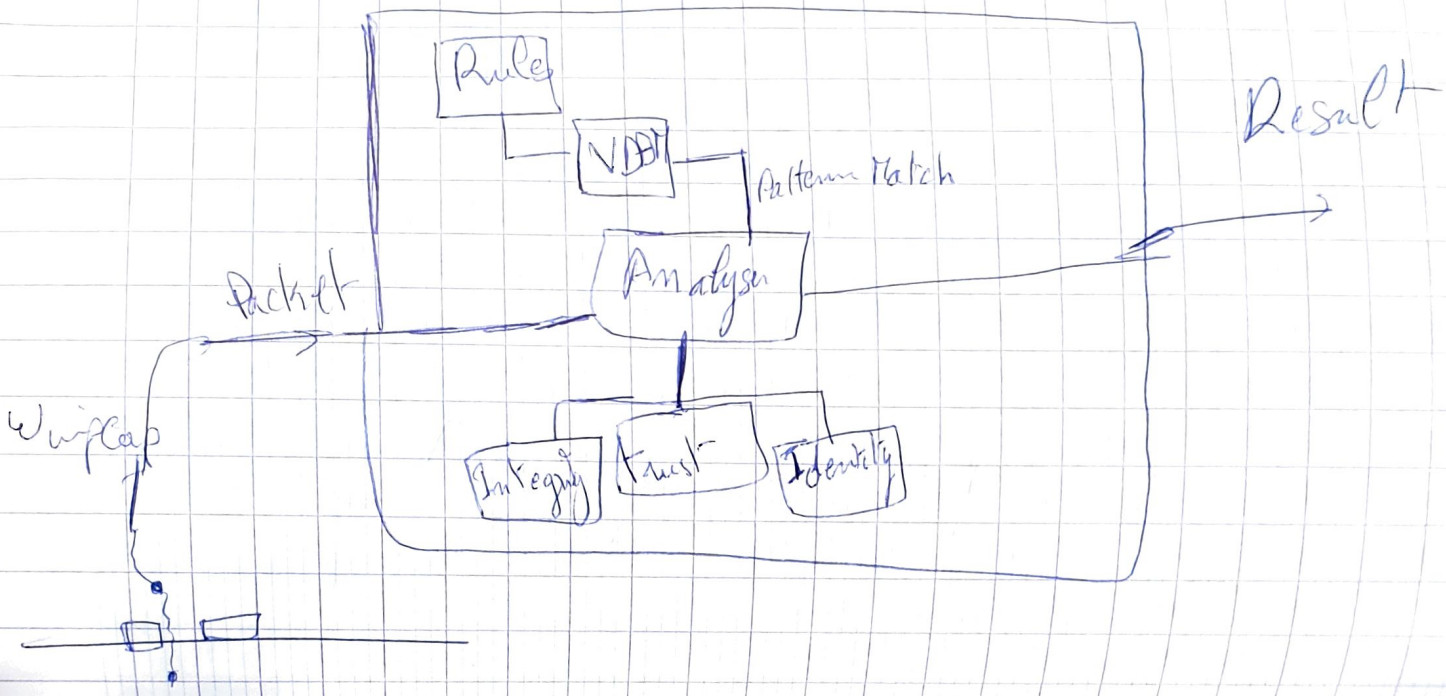
Nikto : VLS server

Sandtrap : HDs

Kaiprot Project Analysis

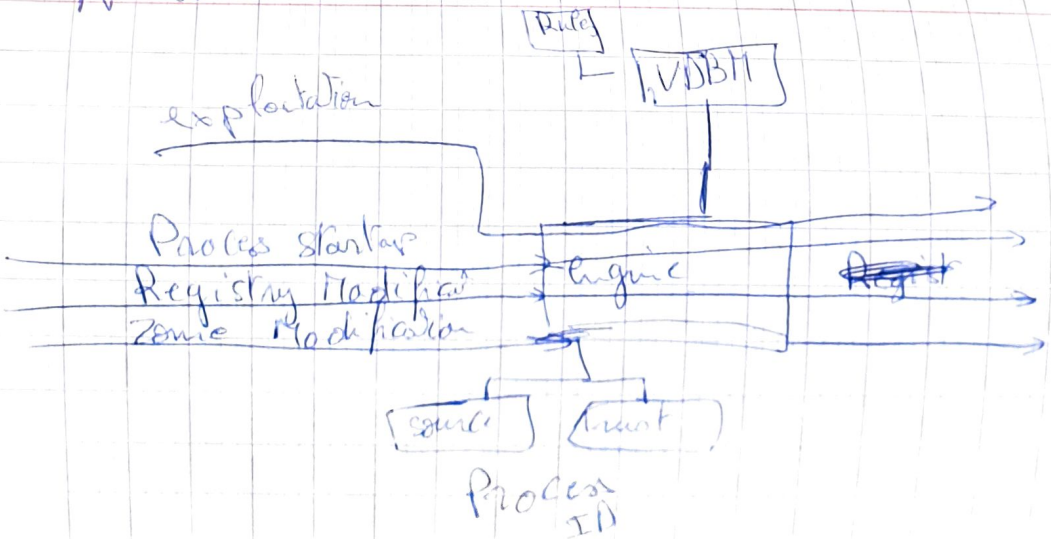
NIDS

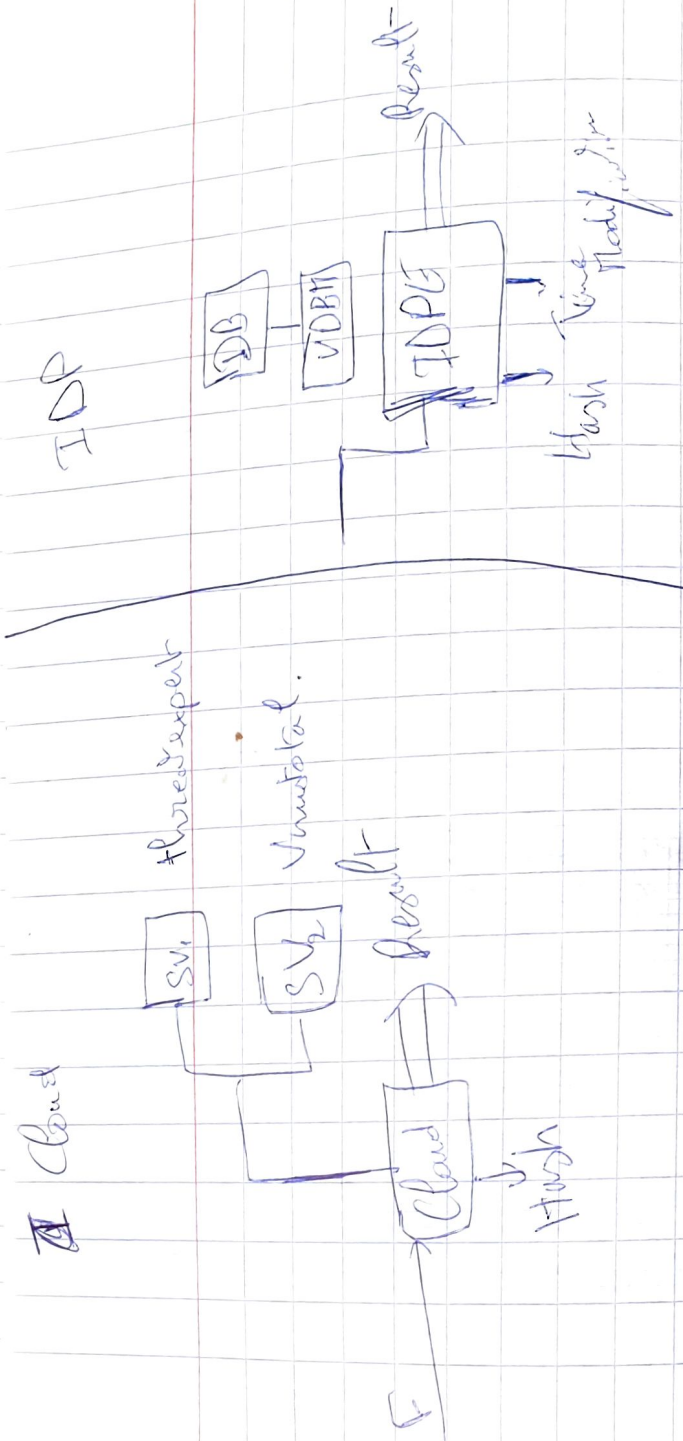
Network - IDS



HIDS

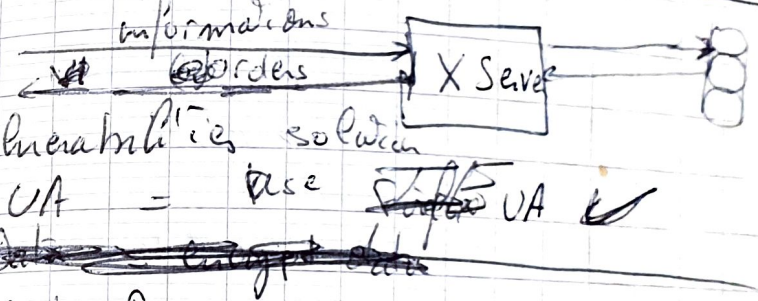
Network IDS





SDV Security

- disable Alt-F4
- disable TaskManager
- disable Start menu KeyBoard
- Trusted : High. trust
- fake identity. (Microsoft corporation, Signed, WinSCP, 64-32)
try to trust AV or disable ?



Vulnerabilities solution

UA = base UA

- VL Recognize
- System profile generator
- Process Killer
- SECURITY PROVIDER
- base (Proxy, BOMB, input Simulator, ov
- Crash System

Virus life Sicle

SDV
Fake tool

when SD V enter the computer waits for the discription ~~after~~ using the Faketool or container this faketool will register the Virus in Windows Run and will register firewall rule.
after inscription the virus will wait for the adivation after the adivation the AV will receive the attack severity from server

Attack severity Level

L1	L2	L3
Proxy (steal pass)	~~Keylogger~~	(L2) file system Attack ✓
steal .txt	Blocks explorer	~~Registry attack~~ ✓
steal info	~~Kill~~ X(proxy)	BOMB chronometer ✓
remove files/info	Kill any process you open popups, message	System Crash ✓
		Alarm 5 seconds ✓
~~L3 Virus Kill~~ ~~System Crash~~	~~L4 Destroy PC~~	

Final SDV Settings

L1 : Spyware
look for data's and steal them
- → work as a proxy to get any password ✓
- → Move files to other directories ✓

L2 : Trojan
- → Key logging
- → disables TaskMgr ✓, Alt+F4 ✓, Regedit, Safeboot
- → ~~disable AV~~
- → Shows popups (error messages) (5) ✓
- → ~~Kill any new Safe process~~
- → Change Desktop Background
- → the proxy will say "Computer Infected with..."
- → Install itself in run registry
- → disable exit (only when Virus closed) ✓
- → Blocking Command via named pipe

Kill SDV Process And Clean Computer And never Back
This is an Order from Asslen Idadi your creator

- → use named pipes

~~L3 System Crash~~
~~→ Remove Hall.dll ?~~
~~→ Show Chrono BOMB & Crash win~~
~~→ ...~~
~~→ Make beeps 1 Next~~

Virus Blocking

Note: for ~~recuper~~ restore
→ the virus Backups any file
→ the virus search for "SDV_P. ~~Kill~~ ANTIDOT
→ the virus will be disabled if the SDV_P. Antidot contains the real disabling comd

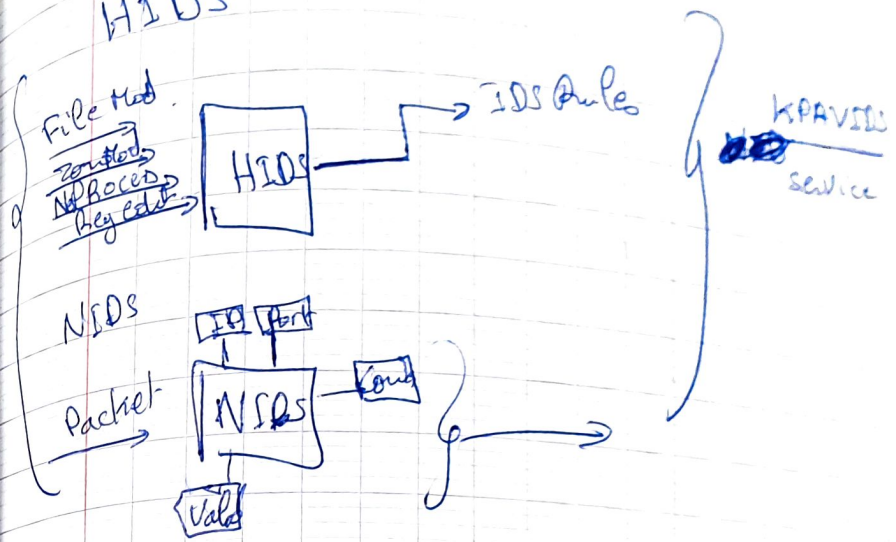
Windows Attack
→ disable control panel
→ disable regedit
→ disable supportinfo.

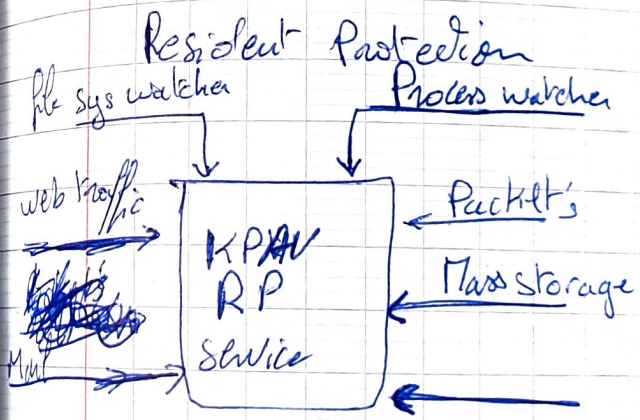
disable many windows functionality as a Program

→ Uninstall AV silently

KAVPROT SS1

HIDS





Genetic Heuristic Engine

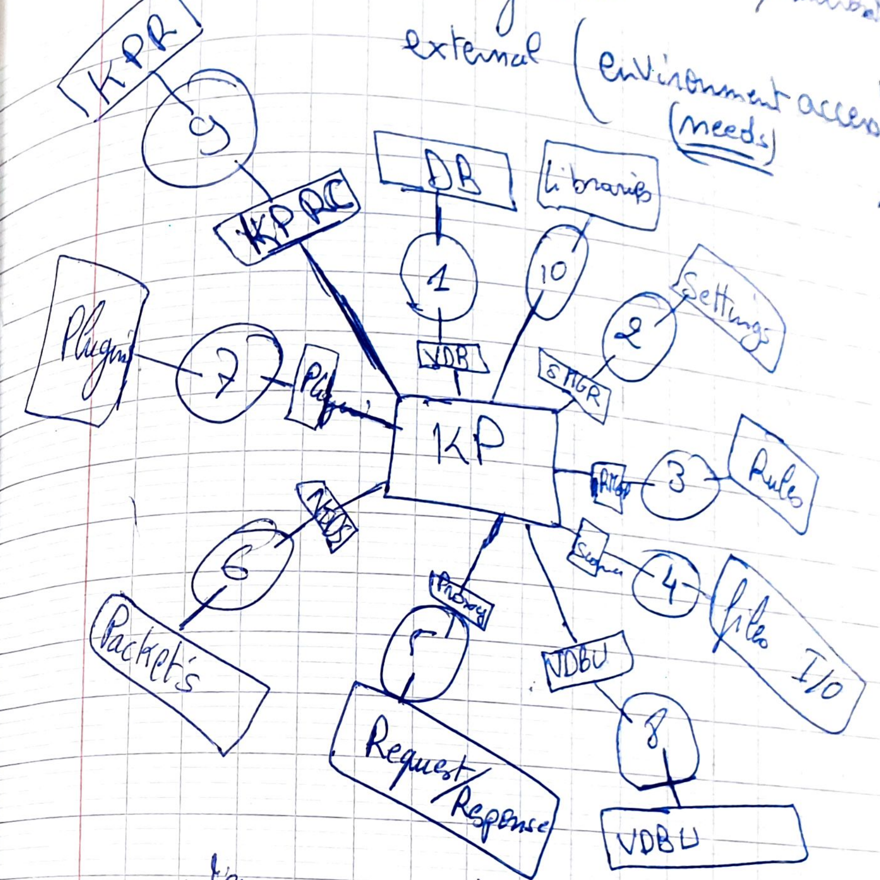
→ Disassembler → IL
→ ASM

→ CODE Parser
P.O.D.L Analyser
→ Program, objectif. Description language Analyser

→ VDBE

Kaupot- and Algorithms Optimization, Vulnerability

external (environment access (needs))



9 communication intrusion KPIB

No	Optimizations	Vulnerability	algo
1	Small Code, FIS, Cache no variable!	injection, access	Password, Monitor
2	no table, nolist, database	access, modification	protection, Anti...
3	low variable		
4	" "	" " "	" " "
5	read code opt, Cleaner memory	file in use, Big Size overflow	Sizelimiter, force scan
6	no container variable	Bad content, overflow	lazer, Detector
7	no container variable	"	" "
8	Single access	Bad plugin (untrusted)	digital Signature
	Download file install	overflow, Bad content	Secure connection VDBU verification

6 days of ideas collections

- Multi-task scan (Async)
- File type scanner (optimized)
- faster sqlite database operations
- Cloud scanner
- Heuristic scanner (ASM, IL)
- SANDBOX
- Exclusion
- safe zone, eagle eye ⇒ HIDS
- pattern matching
- central signal processing
- Assisted Programming language
- DDOS attack, SDV ⇒ counter attack
- SPR, SPS, chatbot ... ⇒ Jane
- IPDTP
- Firewall
- NIDS, WIDS
- Best GUI
- account Management
- Anti-spam
- Mail Defender
- IM Defender
- P2P Defender
- Source code study
- Send SMS

Karspd server

- File trust classifier
- performance counter
- global function control
- self protection
- SCADA agent
- error correction system
- Crash report system
- try-catch distribution (High level layers)
- agent generator