#WHOAMI

Mateus Riad
mateus.riad@poasec.org

POASEC.org
Disseminando segurança, criando cultura.

METASPLOIT

FRAMEWORK

Exploits

- Código responsável por explorar uma determinada vulnerabilidade.

Payloads

- Código que será executado após a exploração para criar e manter a conexão remota.

  Ex: Conexão reversa.

Objetivo

- Desenvolvimento de Exploits
  - Customização e Configuração

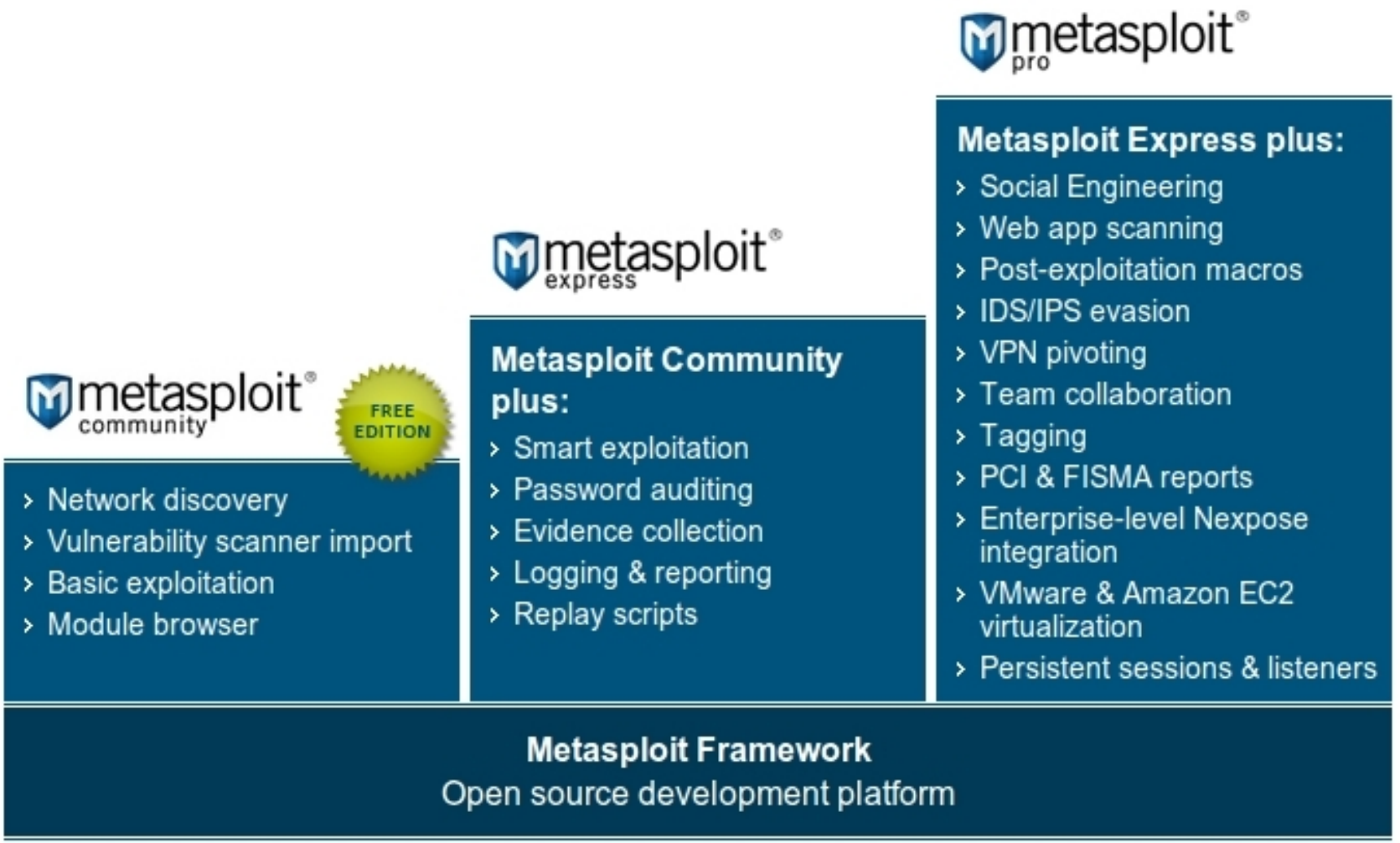
História

- Projeto criado em 2003 - HD Moore
- Inicialmente em Perl
- 2005 – 2007reescrito para Ruby
- 2009 – a Rapid7 adquire Metasploit.

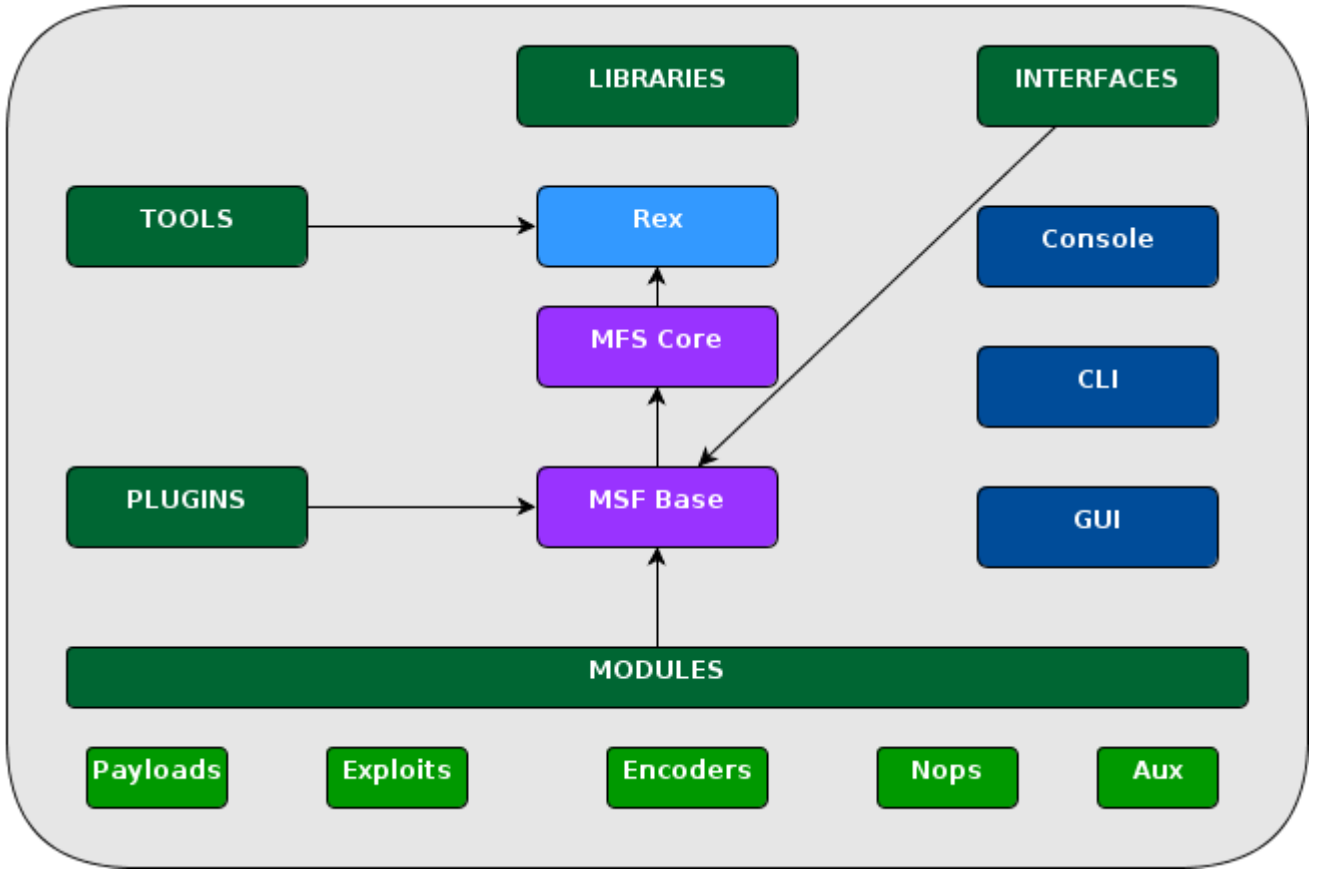
  - Metasploit Express.

  - 2010 - Lançada a versão Comercial MetasploitPro

  - 2011 - Lançado a versão básica Metasploit Community Edition

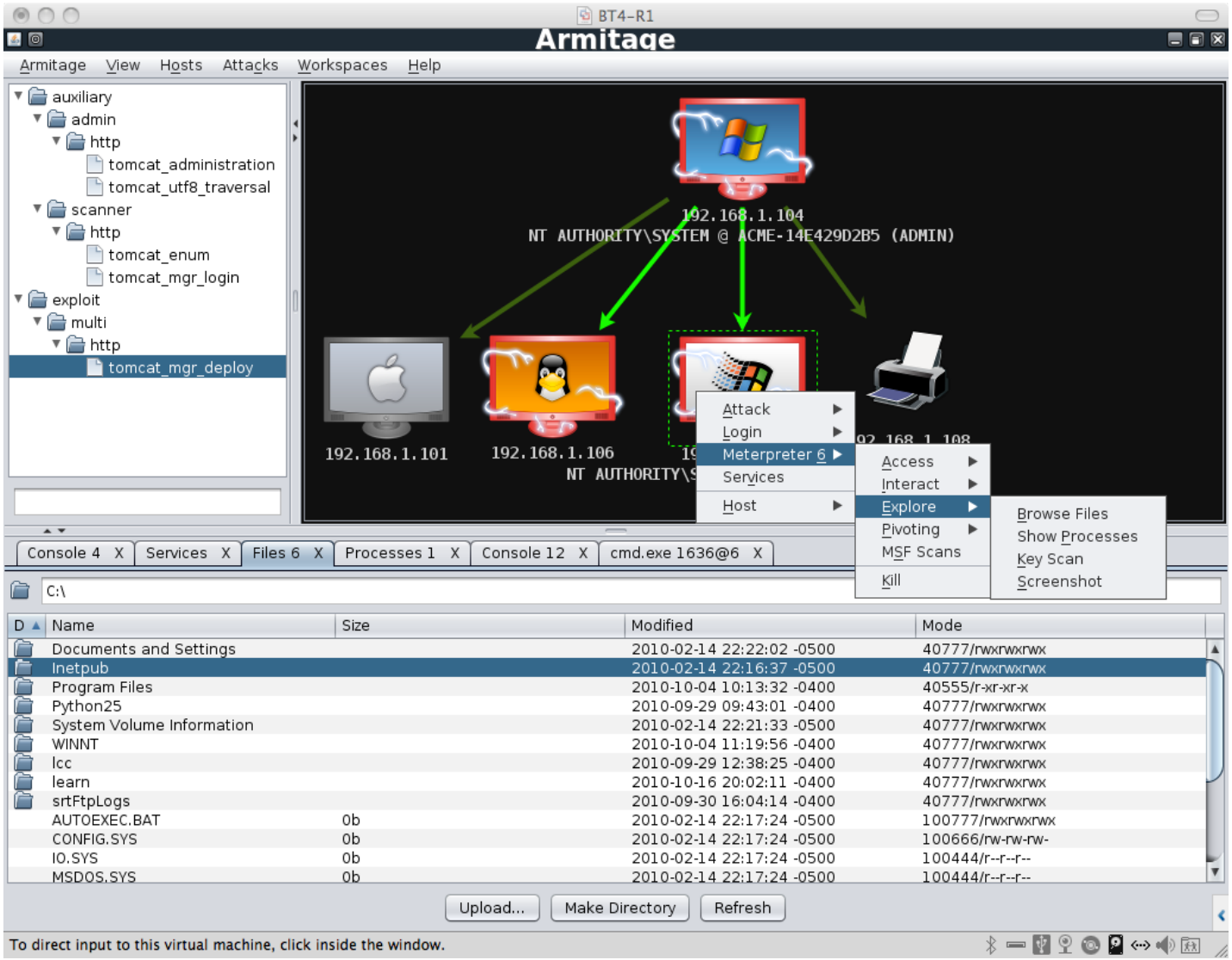

metasploit pro
Metasploit Express plus:
Social Engineering
Web app scanning
Post-exploitation macros
IDS/IPS evasion
VPN pivoting
Team collaboration
Tagging
PCI & FISMA reports
Enterprise-level Nexpose integration
VMware & Amazon EC2 virtualization
Persistent sessions & listeners
metasploit express
Metasploit Community plus:
Smart exploitation
Password auditing
Evidence collection
Logging & reporting
Replay scripts
metasploit community
FREE EDITION
Network discovery
Vulnerability scanner import
Basic exploitation
Module browser
Metasploit Framework
Open source development platform

Estrutura


LIBRARIES
INTERFACES
TOOLS
Rex
Console
MFS Core
CLI
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux

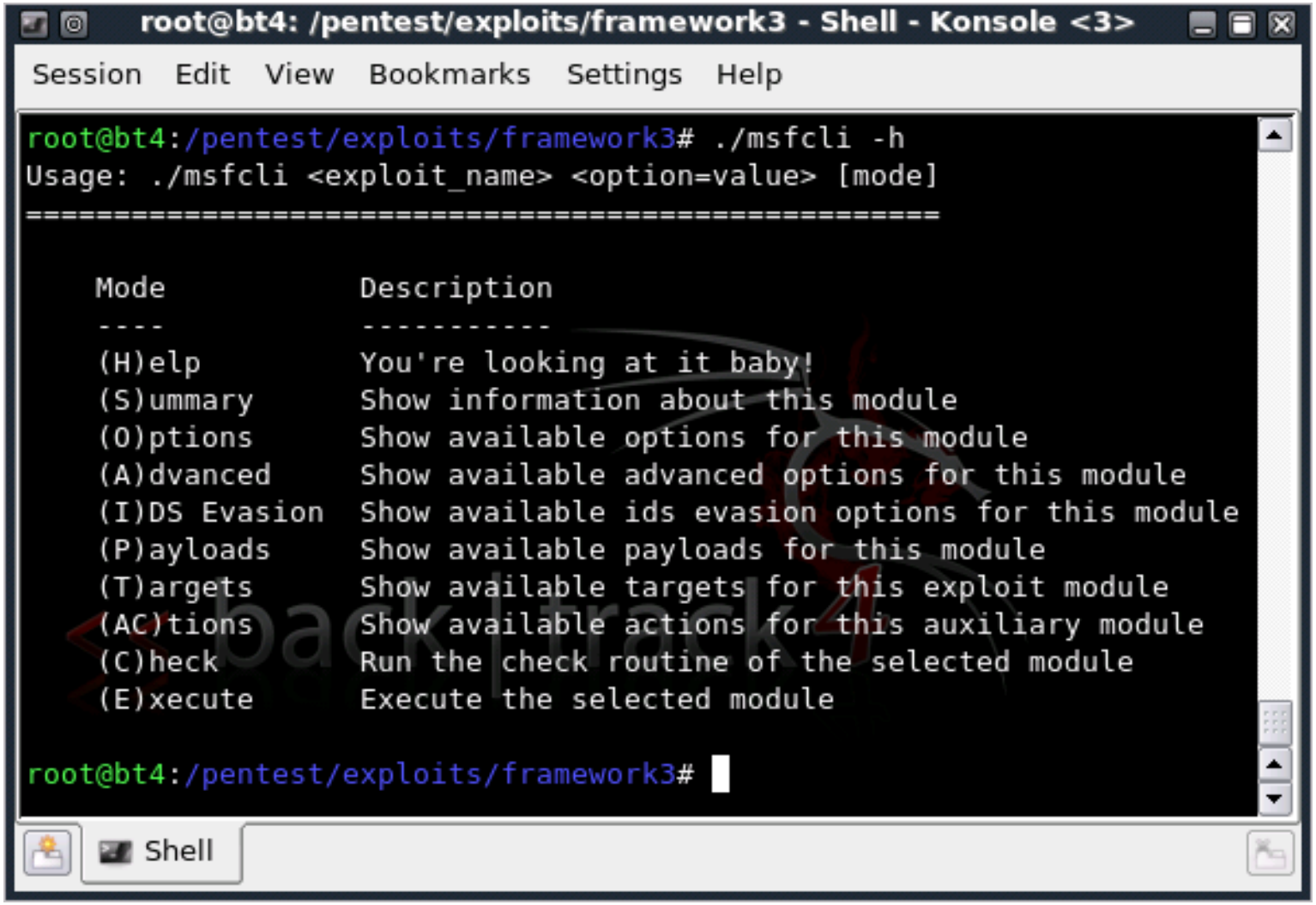
msfweb – Retirada do projeto

- Substituição : Armitage “Point-and-Click”



POASEC.org

Interfaces - msfcli



msfconsole


root@bt:~# msfconsole
=[metasploit v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[814 exploits - 458 auxiliary - 137 post
+ -- --=[248 payloads - 27 encoders - 8 nops
=[svn r14988 updated 58 days ago (2012.03.20)
Warning: This copy of the Metasploit Framework was last updated 58 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306
msf > _

Portabilidade

- Nessus
- Nexpose
- Nmap

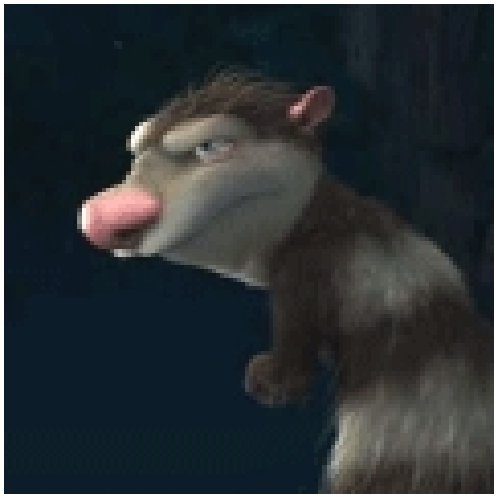
...

Meterpreter

- Gestão de sessões
- Informações de processos
- Manipulação de arquivos
- Execução de comandos

Mantenha-se Atualizado!

“**0-Day**”



[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::AUTHOR
2012-05-21	HP StorageWorks P4000 Virtual SAN Appliance Command Execution	hardware	180		R		D	metasploit
2012-05-19	Active Collab "chat module" <= 2.3.8 Remote PHP Code Injection Exploit	php	385		R		D	metasploit
2012-05-18	Squiggle 1.7 SVG Browser Java Code Execution	multiple	347		R		D	metasploit
2012-05-18	PHP 5.4 Win32 Code Execution	php	903		R		D	0in
2012-05-18	HP VSA Command Execution	hardware	267		R		D	Nicolas Gregoire
2012-05-18	Oracle Weblogic Apache Connector POST Request Buffer Overflow	windows	337		R		D	metasploit
2012-05-13	NEC Backdoor Administrative Account	hardware	942		R		D	iSP0m
2012-05-13	Firefox 8/9 AttributeChildRemoved() Use-After-Free	windows	549		R		D	metasploit

[local exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::AUTHOR
2012-05-21	Foxit Reader 3.0 Open Execute Action Stack Based Buffer Overflow	windows	164		R		D	metasploit
2012-05-19	Vertrigoserv 2.27 Local Privilege Escalation Exploit	windows	560		R		D	X-Cisadane
2012-05-18	SkinCrafter ActiveX Control version 3.0 Buffer Overflow	windows	409		R		D	saurabh sharma
2012-05-16	Linux Kernel 3.3.x <= 3.3.4 Buffer overflow in HFS plus filesystem	linux	975		R		D	Timo Warns
2012-05-16	LAN Messenger v1.2.28 - Persistent Software Vulnerability	windows	444		R		D	Benjamin K.M.
2012-05-13	ABBS Media Player 3.1 Buffer Overflow Exploit (SEH)	windows	344		R		D	Caddy-Dz
2012-05-12	AnvSoft Any Video Converter 4.3.6 Unicode Buffer Overflow	windows	384		R		D	h1ch4m
2012-05-11	Adobe Photoshop CS5.1 U3D.8BI Collada Asset Elements Stack Overflow	windows	733		R		D	rgod

[webapps / 0day]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::AUTHOR
2012-05-21	Aholattafun Creative Solutions SQL Injection Vulnerabilities	php	353		R		D	Becax
2012-05-21	Vanilla Forums About Me Plugin Persistant XSS	php	186		R		D	Henry Hoggard
2012-05-20	Ajaxmint-Gallery v1.0 <= CSRF Change Admin Password	php	384		R		D	KedAns-Dz
2012-05-20	Concrete CMS v5.5 <= Multiple Vulnerabilities	php	393		R		D	KedAns-Dz
2012-05-20	PHP CGI Argument Injection Remote Exploit (PHP Version)	php	642		R		D	Mostafa Azizi
2012-05-20	Land.Net SQL injection Vulnerability	php	622		R	G	D	k2ll33d
2012-05-19	CHICCO SnoopyClub - SQL Injection / XSS / LFI Vulnerabilties	php	594		R	G	D	the_cyber_nuxbie
2012-05-19	FreeNAC version 3.02 SQL Injection / XSS Vulnerabilties	php	360		R		D	Blake

[dos / poc]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK				-::AUTHOR
2012-05-21	PHP <= 5.4.3 (com_event_sink) Denial of Service	php	196		R		D	condis
2012-05-21	PHP <= 5.4.3 wddx_serialize_* / stream_bucket_* Object Null Ptr Dereference	php	182		R		D	condis
2012-05-21	Real-DRAW PRO 5.2.4 Import File Crash	windows	135		R		D	Ahmed Elhady
2012-05-21	DVD-Lab Studio 1.25 DAL File Open Crash	windows	151		R		D	Ahmed Elhady
2012-05-20	Mozilla FireFox 12.0 Memory Corruption (with ROP)	windows	1015		R	X	D	KedAns-Dz
2012-05-19	PHP 5.3.11 (win) Local Denial Of Service	php	823		R		D	Angel Injection
2012-05-18	SkinCrafter 3.0 Buffer Overflow	windows	257		R	X	D	saurabh sharma
2012-05-15	Multimedia Builder 4.9.8 Malicious mef Crash	windows	341		R		D	Ahmed Elhady

Pentest

- Discovery
- Enumeration
- Vulnerability Identification
- Exploitation and Launching of Attacks
- Escalation
- Reporting

Demonstração

POASEC.org

Muito Obrigado!

Mateus Riad

mateus.riad@poasec.org