METASPLOIT

Martin Kralev & Dmitrii Strizhkov

Overview

- What is Metasploit?
- Brief History
- Architecture & Structure
- Workflow
- *Demo*

What is Metasploit?

What is Metasploit?

- Computer Security Project → Penetration Testing
- Security tools and exploits
- Automating the exploitation process and delivers payload

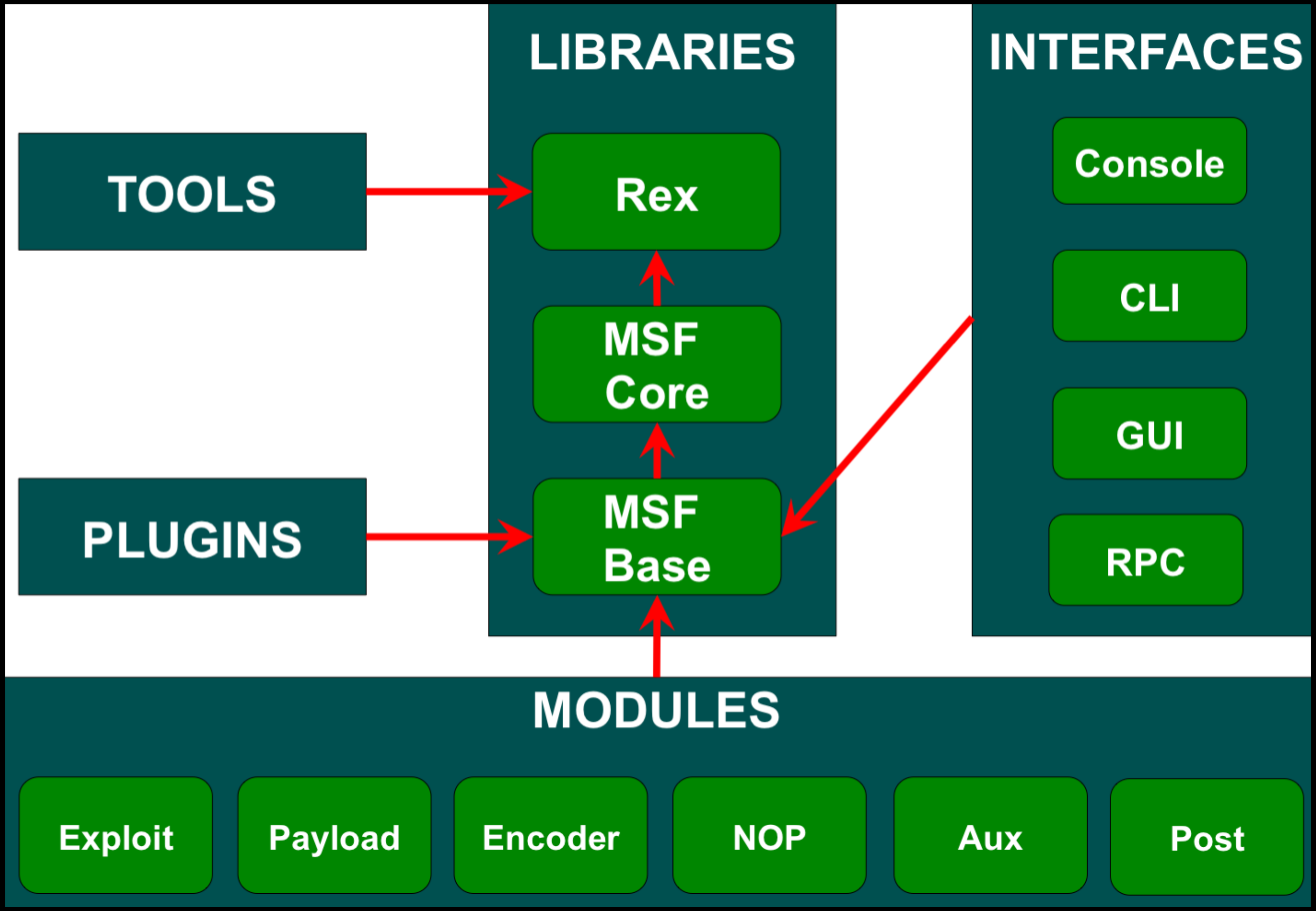
History

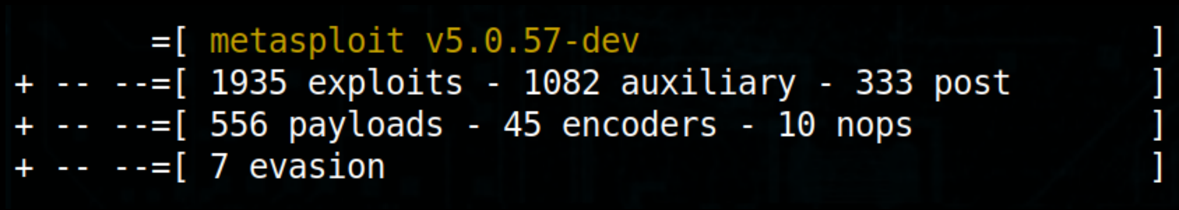
Metasploit History

- Developed by H. D. Moore in 2003
- Originally written as a portable network tool using Perl
- Rewritten in Ruby
- Owned by Rapid7

Architecture & Structure

Architecture & Structure

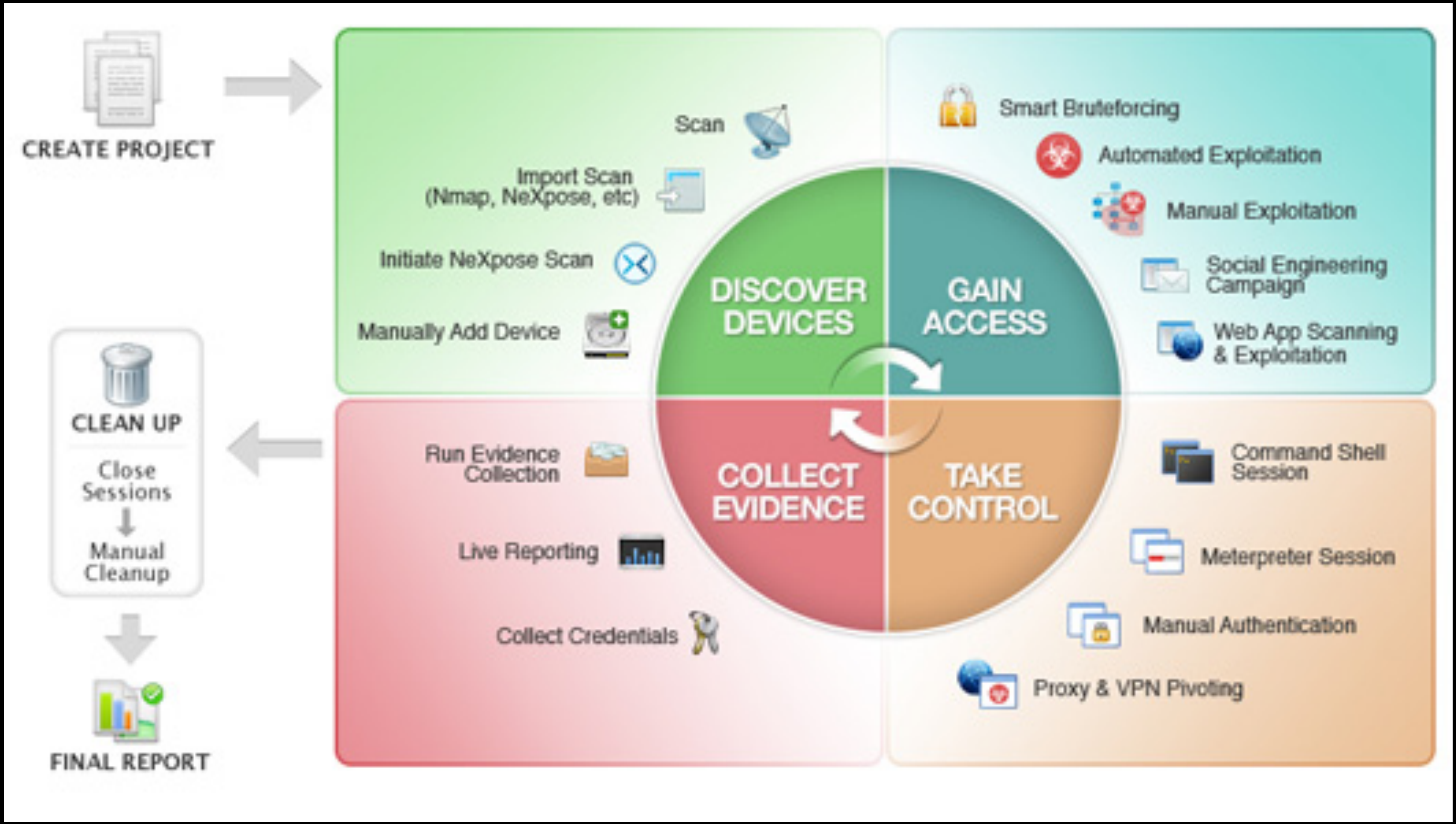




```
        =[ metasploit v5.0.57-dev                          ]
+ -- --=[ 1935 exploits - 1082 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                        ]
```

Workflow

Workflow


CREATE PROJECT
Scan
Import Scan
(Nmap, NeXpose, etc)
Initiate NeXpose Scan
Manually Add Device
DISCOVER DEVICES
GAIN ACCESS
Smart Bruteforcing
Automated Exploitation
Manual Exploitation
Social Engineering Campaign
Web App Scanning & Exploitation
CLEAN UP
Close Sessions
Manual Cleanup
FINAL REPORT
Run Evidence Collection
Live Reporting
Collect Credentials
COLLECT EVIDENCE
TAKE CONTROL
Command Shell Session
Meterpreter Session
Manual Authentication
Proxy & VPN Pivoting

Metasploit Controls

Metasploit Controls

```
$ sudo msfconsole
```

```
> help
```

```
> search type:exploit cve:2010 platform:unix irc
```

Metasploit Controls

```
> use EXPLOIT (module name: syntax xxx/xxx/xxx/)

      show
            options
            payloads
            targets
            info

      set ATTRIBUTE (or setg for global)

      check

      exploit

      back
```

Demo

Usage Summary

Usage Summary

1. Choose an exploit
2. Configure the parameters
3. Check if it will work
4. Execute
5. ???
6. Profit

Questions?