GoLismero

v2.0
Cheat Sheet

http://golismero-project.com | @golismero_pro

Quick start

Installation (from git):
```
git clone https://github.com/golismero/golismero golismero
```
Global commands.
```
golismero {SCAN|PROFILES|PLUGINS|INFO|REPORT|IMPORT|DUMP|UPDATE}
```

Scanning

Quick scan:
```
golismero.py scan TARGET
golismero.py scan 10.0.0.0/24 172.16.0.0/24 TARGET
```
List available profiles:
```
golismero.py profiles
```
Custom plugins setup:
```
golismero.py scan -e spider -e plecost -e dns* TARGET
```
Plugin parameters:
```
golismero.py scan -a openvas:port=9182 -a openvas:user=tor  TARGET
golismero.py scan -a openvas:profile="My new profile" TARGET
```
Audit name and results database:
```
golismero.py scan --audit-name my_audit -db my_database.db TARGET
```
Without database and increasing debug level:
```
golismero.py scan -nd -vv TARGET
```
Setting proxy:
```
golismero.py scan -pu USER -pp PASS -pa ADDRESS -pn PORT TARGET
```
Following redirects (or only one) and set max depth crawling:
```
golismero.py scan --follow-redirects --depth 2 TARGET
golismero.py scan --follow-first --depth 4 TARGET
```
Performance and networks options:
```
golismero.py scan --max-concurrent 10 --max-connections 25 TARGET
```
Set scope and limits:
```
golismero.py scan --max-links 95 --allow-subdomains --parent TARGET
golismero.py scan --forbid-subdomains --no-parent TARGET
```
Session management:
```
golismero.py scan --cookie "COOKIE_VAL" --user-agent random TARGET
golismero.py scan --cookie-file FILE_PATH.jar TARGET
```
Set profile:
```
golismero.py scan --profile quick TARGET
```

Manage plugins

List available plugins:
```
golismero.py plugins
```
Display plugin details:
```
golismero.py info openvas
```

Reporting

Available formats: .html | .json | .csv | .xml | .yaml | .rst | .txt

Generate html report:
```
golismero.py scan WEBSITE -o report.html
```
Generate multiple reports:
```
golismero.py report -o report.html -db info.db
```
Generate report from database:
```
golismero.py report -o r.xml -o r.txt -o r.rst
```

Importing results

Import information from other tools:
```
golismero.py import -i openvas_results.xml
```
Import information from other tools:
```
golismero.py report -i ov.xml -o res.html
```

SQL Database import/export

Import information from other tools:
```
golismero.py dump -db example.db -o dump.sql
```
Import information from other tools:
```
golismero.py load -i dump.sql
```

GOLISMERO + python + GPL

Real multi platform

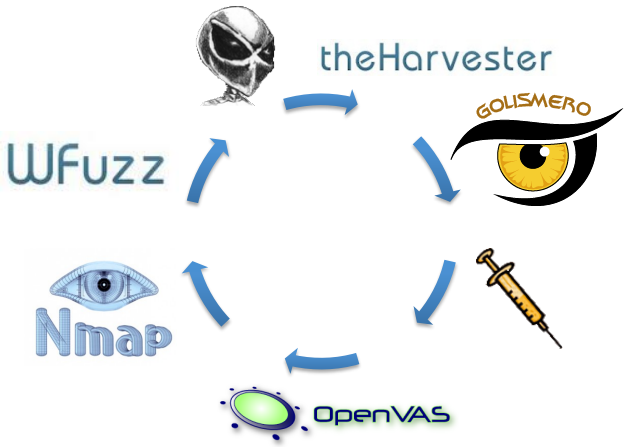
Complete toolbox:

- OpenVAS
- nmap
- XSSer
- SQLmap
- Theharvester
- Punkspider
- Spiderfoot
- SSLscan
- Wfuzz
- Dnsrecon
- nmap
- ….

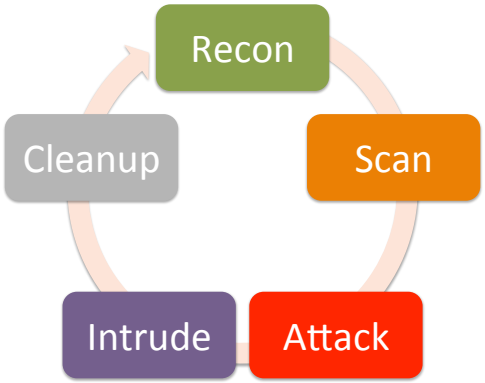
Basic usage is easy…

```
5. Shell
Shell ⌘1
GoLismero# python golismero.py scan  http://example.com -o report.html
```

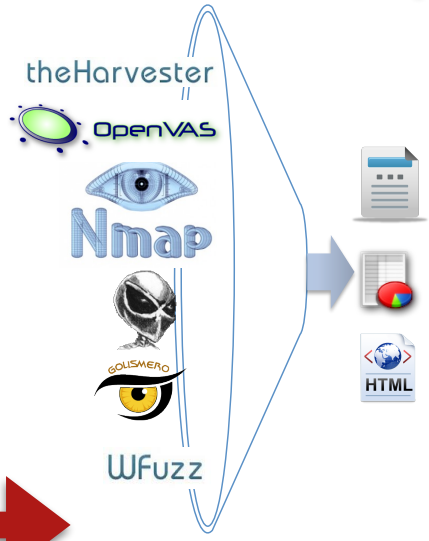
Results feedback model



Audit steps well defined



Unified results



Pretty report, with responsive design.