Information Gathering

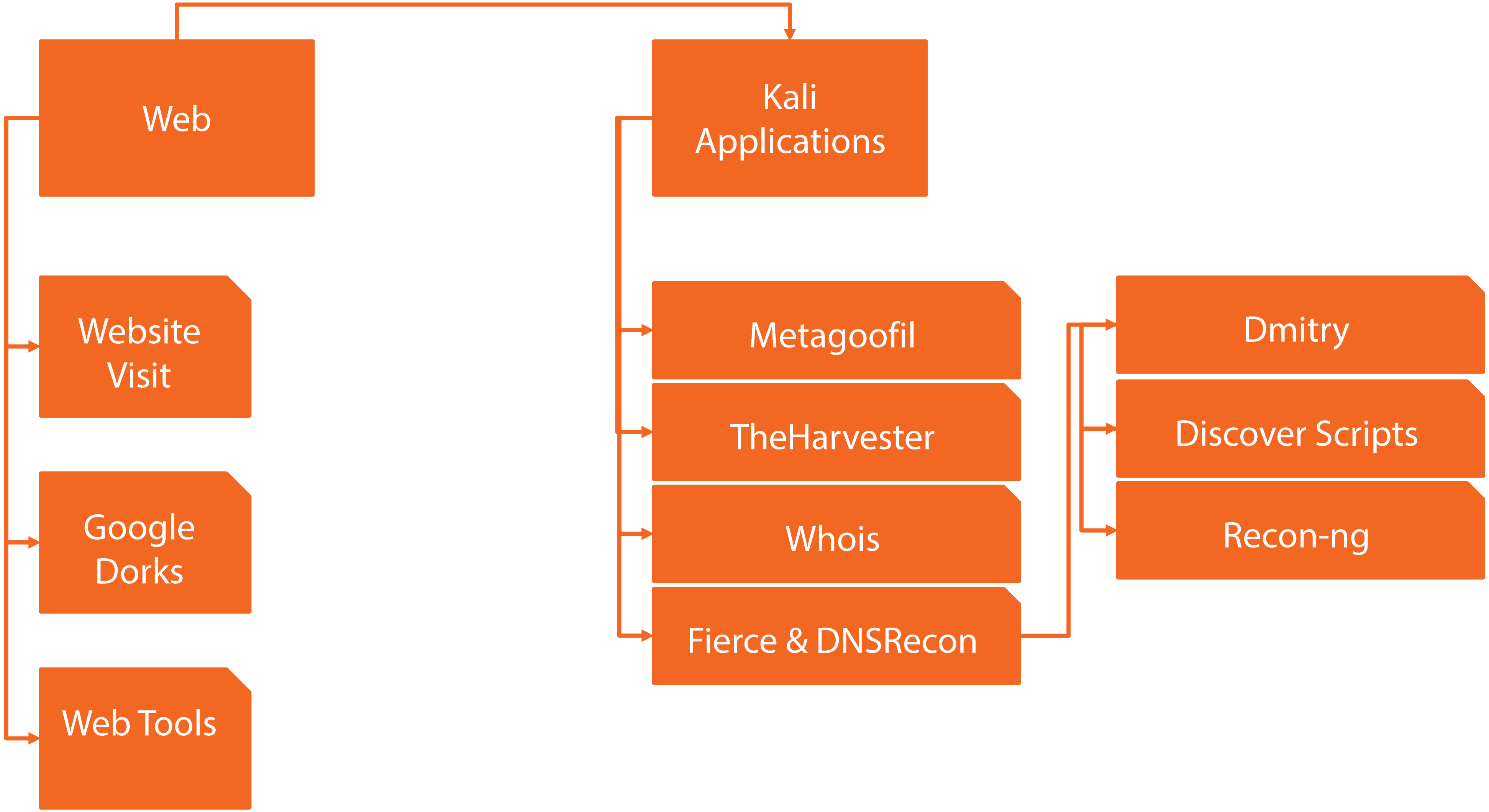
Author Gus Khawaja

Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com

Gathering Information Checklist

Workflow


Web
Website Visit
Google Dorks
Web Tools
Kali Applications
Metagoofil
TheHarvester
Whois
Fierce & DNSRecon
Dmitry
Discover Scripts
Recon-ng

Checklist

Other Techniques

- Geographical location
- Parent Company/ Acquisition
- Language && Culture
- Cached Contents
- Yellow Pages
- Social Networks
- Visit the Client Premises

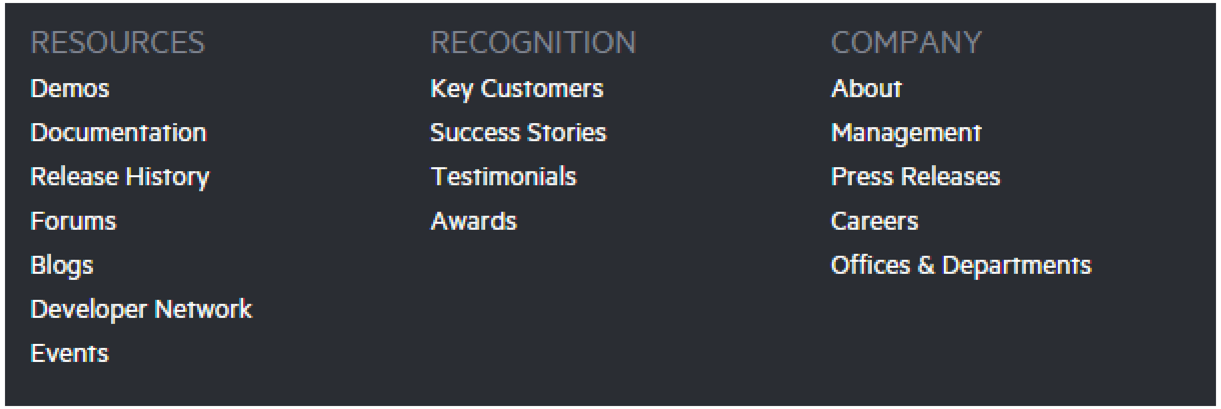
Information Gathering

KeepNote

Information Gathering

Website Visit

Demo



RESOURCES

Demos
Documentation
Release History
Forums
Blogs
Developer Network
Events

RECOGNITION

Key Customers
Success Stories
Testimonials
Awards

COMPANY

About
Management
Press Releases
Careers
Offices & Departments

Information Gathering

Google Hacking Database

(Google Dorks)

Google Filters

Operator	Syntax
cache	**cache**: *URL [string]*
filetype	**filetype**: *[type]*
info	**info**: *[string]*
intitle	**intitle**: *[string]*
inurl	**inurl**: *[string]*
site	**site**: *[domain/Website][string]*

Information Gathering

Web Tools

Demo

www.dnsstuff.com

Information Gathering

Documents Metadata

Documents Metadata

Examples

- Owner
- Date & Time of Creation/Modification
- Network Location
- Geolocation

Demo

Metagoofil

Information Gathering

Email Addresses & Hosts

Demo

TheHarvester

Information Gathering

Whois

Information Gathering

DNS Reconnaissance

Information Gathering

Deepmagic Information Gathering Tool (Dmitry)

Information Gathering

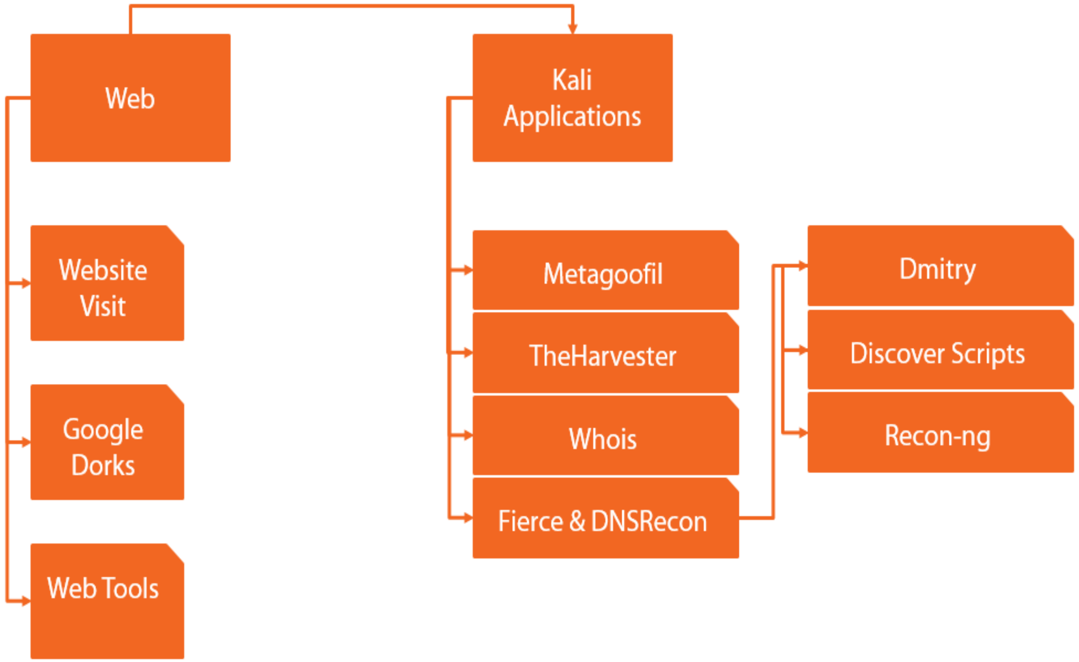
Discover Scripts

Information Gathering

Recon-ng

Summary

Workflow


Web
Website Visit
Google Dorks
Web Tools
Kali Applications
Metagoofil
TheHarvester
Whois
Fierce & DNSRecon
Dmitry
Discover Scripts
Recon-ng