Website Penetration Test

Author Gus Khawaja

Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com

Website Penetration Test Checklist

Checklist

- ✓ Reconnaissance (previously described)
- ✓ Web application firewall scanning
- ✓ Load balancing check
- ✓ Web crawling
- ✓ Copy the website locally
- ✓ Scan for CMS
- ✓ Scan for SSL

Checklist

- ✓ Web specific vulnerabilities scan
- ✓ Sessions tokens test
- ✓ Exploiting SQL injection
- ✓ Maintaining access
- ✓ Denial Of Service (DOS)

Website Penetration Test

Web Application Firewall(WAF)

Demo

wafw00f

Website Penetration Test

Load Balancing Check

Demo

lbd

Website Penetration Test

Web Crawling

Findings

Admin portals

Config files

Backup copies

Admin notes

Confidential information

Source code

Kali Crawlers

Burp suite

Dirbuster

OWASP-ZAP

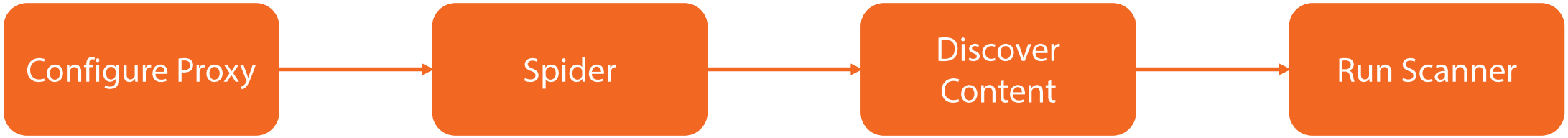
Vega

Webscarab

Webslayer

Demo

Burp Suite



Website Penetration Test

Burp Proxy

Burp Proxy

Website Penetration Test

Burp Target

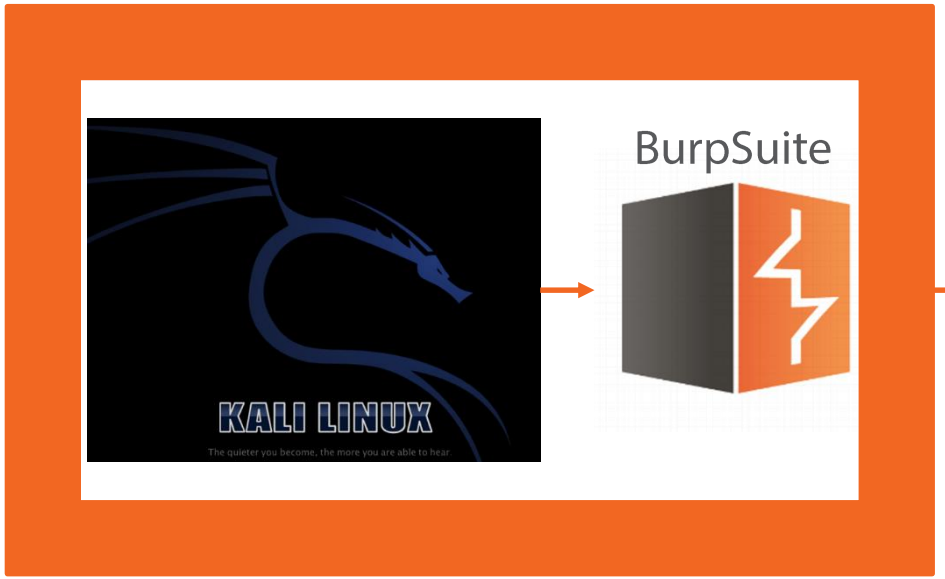
Website Penetration Test

Burp Spider

Website Penetration Test

Burp Discover Content

Attack



http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Website Penetration Test

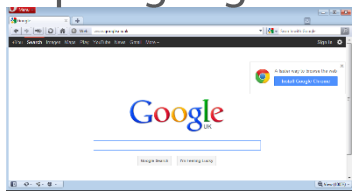
Copy website

Website Penetration Test

SSL Scan (Demo sslscan)

SSL

https://google.com



Hello Server

Hello Client (SSL Ver + SessionID+ Certificate)

Hello Done

Symmetric Encryption Key

Hashed Message

Finish

Google™

Website Penetration Test

CMS Scan

Website Penetration Test

Web Specific Vulnerabilities Scan

Website Penetration Test

Sessions Tokens

Website Penetration Test

Input Validation

Website Penetration Test

Exploiting SQL Injection

Website Penetration Test

Maintaining Access

Demo

Weevely

File browsing

File transfer

Auditing

Compromising SQL servers

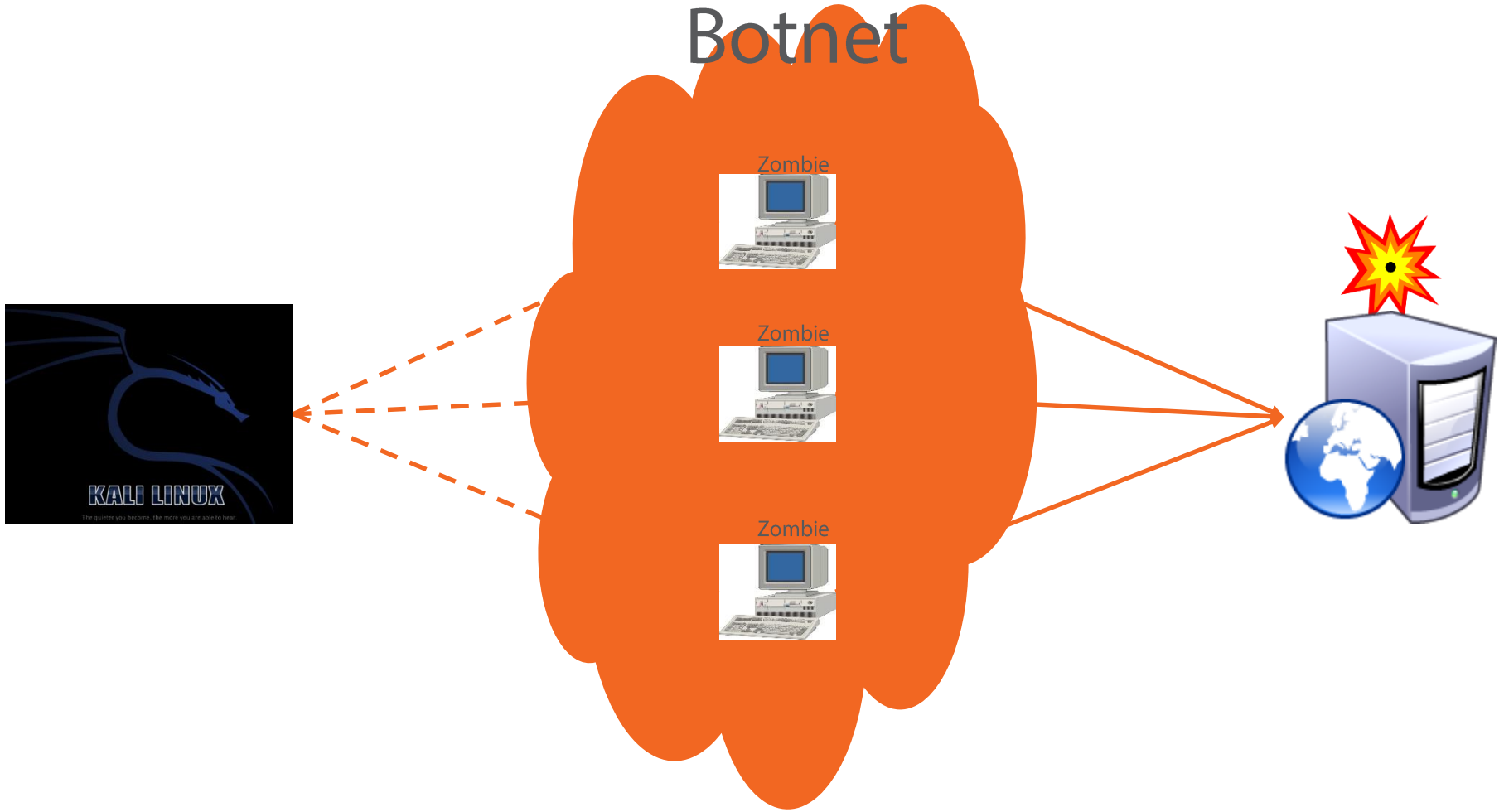
Reverse TCP shells

Command execution

Website Penetration Test

DOS

DDOS



Demo

Low Orbit Ion Cannon (LOIC)

Summary

Sslscan

Wpscan

Wafw00f

Ibd

Burp suite!!!

HTTrack

Sqlmap

Weevely

Low Orbit Ion Cannon