



Kali

Linux

Matej Papaj 1.V

Čo je kali linux

OS
odvodený
od debianu
urč. na
penetračné
testovanie
a analýzu

Obsahuje
stovky
nástrojov na
úlohy
bezpečnosti

open-source
distribúcia

prepísany
BackTrack
linux

Historia

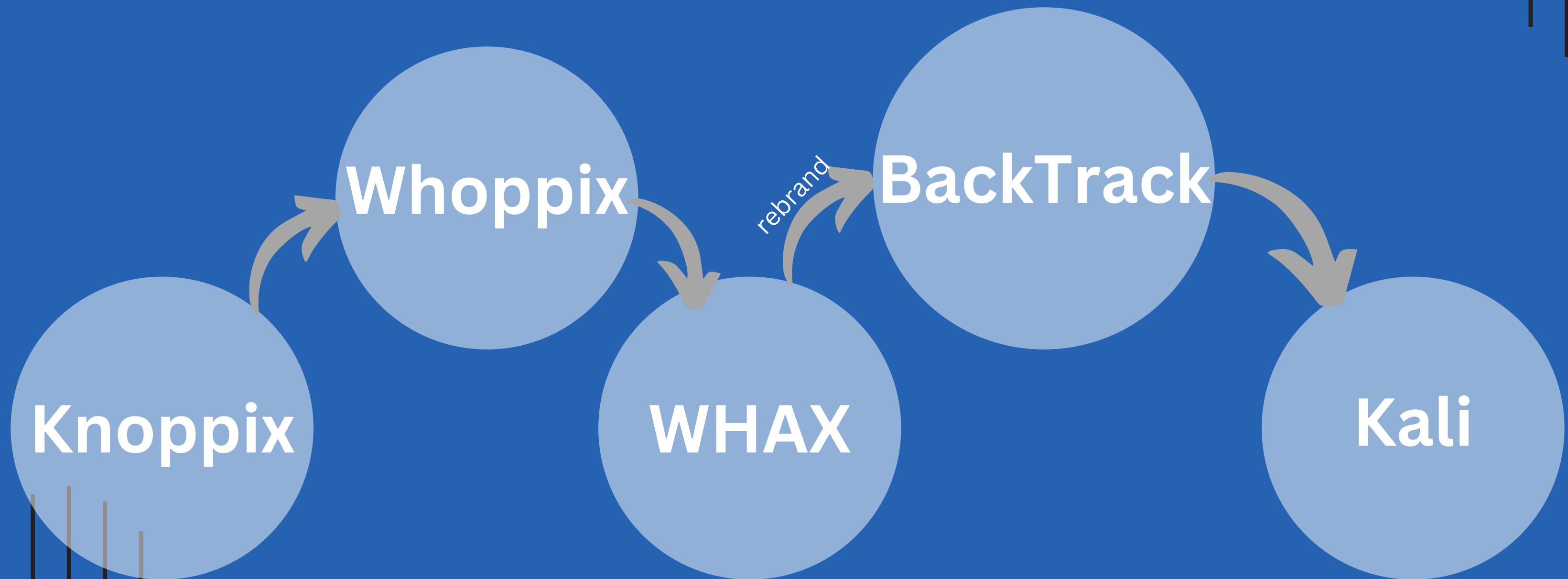
knoppix, 1 linux

knoppix bol potom **prerobený na whoppix**
a **potom na WHAX.**

Whax bol premenovaný na BackTrack
a dlho, takmer 7 rokov, vládol ako voľba pentesterov
a hackerov.

V roku **2013 ho nahradil kali**

evolucia kali



Vlastnosti

1

obsahuje viac ako 600 nástrojov na penetračné testovanie

2

bezplatný a otvorený zdrojový kód

3

má monolitický typ jadra (celý OS pracuje v priestore jadra)

4

úplne prispôsobiteľný

5

Flexibilita (podpora zariadení fungujúce na ARM)

niektoré z nástrojov kali linux

nástroje na zhromažďovanie informácií

-
- dnsdict6
 - dnsenum
 - dnsmap
 - dnsrecon
 - dnsrevenue6
 - dnstracer
 - dnswalk
 - fierce
 - maltego
 - nmap
 - urlcrazy
-

nmap

vdďaka množstvu parametrov je ako švajčiarsky armádny nôž na všetky situácie, v ktorých je potrebná identifikácia siete.

skenuje hostiteľa, snaží sa identifikovať nainštalované služby

```
(root@kali)-[/home/kali]
# nmap -sS -sV 192.168.0.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-02 08:39 EDT
Nmap scan report for 192.168.0.117
Host is up (0.0012s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds

[/home/kali]
```



```
(kali㉿kali)-[/root]
$ dnstracer www.pornhub.com
Tracing to www.pornhub.com[a] via 10.0.2.3, maximum of 3 retries
10.0.2.3 (10.0.2.3) Got answer [received type is cname]
|__ ns12.digicertdns.com [pornhub.com] (2600:1802:0002:0000:0000:0000:0001:001f) * * *
|__ ns12.digicertdns.com [pornhub.com] (208.80.126.159) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.org [pornhub.com] (156.154.143.3) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.org [pornhub.com] (2610:00a1:1004:0000:0000:0000:0000:0003) * * *
|__ ns14.digicertdns.net [pornhub.com] (2600:1802:0004:0000:0000:0000:0001:001f) * * *
|__ ns14.digicertdns.net [pornhub.com] (208.80.127.159) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.net [pornhub.com] (2610:00a1:1002:0000:0000:0000:0000:0003) * * *
|__ sdns3.ultradns.net [pornhub.com] (156.154.141.3) Got authoritative answer [received type is cname]
|__ ns11.digicertdns.com [pornhub.com] (2600:1801:0001:0000:0000:0000:0001:001f) * * *
|__ ns11.digicertdns.com [pornhub.com] (208.80.124.159) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.com [pornhub.com] (2610:00a1:1001:0000:0000:0000:0000:0003) * * *
|__ sdns3.ultradns.com [pornhub.com] (156.154.140.3) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.biz [pornhub.com] (156.154.142.3) Got authoritative answer [received type is cname]
|__ sdns3.ultradns.biz [pornhub.com] (2610:00a1:1003:0000:0000:0000:0000:0003) * * *
|__ ns13.digicertdns.net [pornhub.com] (2600:1801:0003:0000:0000:0000:0001:001f) * * *
|__ ns13.digicertdns.net [pornhub.com] (208.80.125.159) Got authoritative answer [received type is cname]

(kali㉿kali)-[/root]
$
```

dnstracer

umožňuje sledovať servery DNS na
zdroj

určuje, odkiaľ daný server s názvom
domény DNS získava informácie, a
sleduje reťazec serverov DNS späť k
serverom, ktoré poznajú údaje.

zhromažďovanie informácií - identifikácia IDS/IPS

-
- fragroute
 - fragrouter
 - wafw00f
-

wafw00f

identifikuje vzdialené webové
aplikačné firewally

```
(root@kali)-[~]  
wafw00f www.pornhub.com
```



~ WAFW00F : v2.2.0 ~

The Web Application Firewall Fingerprinting Toolkit

```
Checking https://www.pornhub.com  
Generic Detection results:  
No WAF detected by the generic detection  
Number of requests: 7
```

```
(root@kali)-[~]  
# wafw00f www.telekom.sk
```



~ WAFW00F : v2.2.0 ~

The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking https://www.telekom.sk  
[+] The site https://www.telekom.sk is behind BIG-IP AppSec Manager (F5 Networks) WAF.  
[~] Number of requests: 2
```

webové aplikačné firewally (WAF)
možno odhaliť prostredníctvom
scenárov testovania
podnetov/odpovedí

skenery zraniteľnosti webu

-
- burpsuite
 - cadaver
 - davtest
 - deblaze
 - fimap
 - grabber
 - joomscan
 - nikto
 - padbuster
 - proxystrike
 - xsser
 - skipfish
 - sqlmap
 - vega
 - w3af
 - wapiti
 - webscarab
 - webshag-cli
 - webshaggui
 - websploit
 - wpscan
 - zaproxy
-

```
(root@kali)~[~]
# wapiti -u http://www.pornhub.com
```

WAPITI3

```
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Be careful! New moon tonight.
[*] Saving scan state, please wait ...
```

Note

This scan has been saved in the file /root/.wapiti/scans/www.pornhub.com_folder_969855f1.db

[*] Wapiti found 1 URLs and forms during the scan

[*] Loading modules:

backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, rec, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web...

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
OK
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
OK

[*] Launching module cookieflags
Checking cookie : platform
HttpOnly flag is not set in the cookie : platform
Checking cookie : ss
HttpOnly flag is not set in the cookie : ss
Checking cookie : __s
HttpOnly flag is not set in the cookie : __s
Checking cookie : __l
HttpOnly flag is not set in the cookie : __l

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=1ro8gk for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

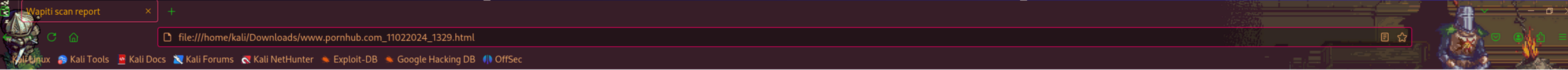
Report

A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/www.pornhub.com_11022024_1329.html with a browser to see this report.

wapiti

umožňuje auditovať zabezpečenie
webovej aplikácie.
vykonáva kontrolu „black-box“

odpoved' od wapiti



Wapiti vulnerability report

Target: <http://www.pornhub.com/>

Date of the scan: Sat, 02 Nov 2024 13:29:35 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	2
HttpOnly Flag cookie	4
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

[Description](#) [HTTP Request](#) [cURL command line](#)

CSP is not set

útoky na hesla

- oclhashcat-lite
- oclhashcat-plus
- pyrit

zneužívania databázy

- bbqsql
- sqlninja
- sqlsus

webové aplikácie fuzzlers

- powerfuzzer
- webscarab
- webslayer
- websploit
- wfuzz
- xsser
- zaproxy
- burpsuite

bezdrôtové útoky: nástroje

bluetooth

- bluelog
- bluemaho
- blueranger
- btscanner
- fang
- spooftooph

zdroj informácií

https://www.slideshare.net/slideshow/tools-kali/56735384?from_search=13#270

<https://www.kali.org/>

<https://www.kali.org/docs/>

<https://www.kali.org/tools/>

<https://www.slideshare.net/slideshow/kali-linux-57428333/57428333#16>

<https://en.wikipedia.org/wiki/Fuzzing>

https://en.wikipedia.org/wiki/Kali_Linux

Ďakujem za
pozornosť