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

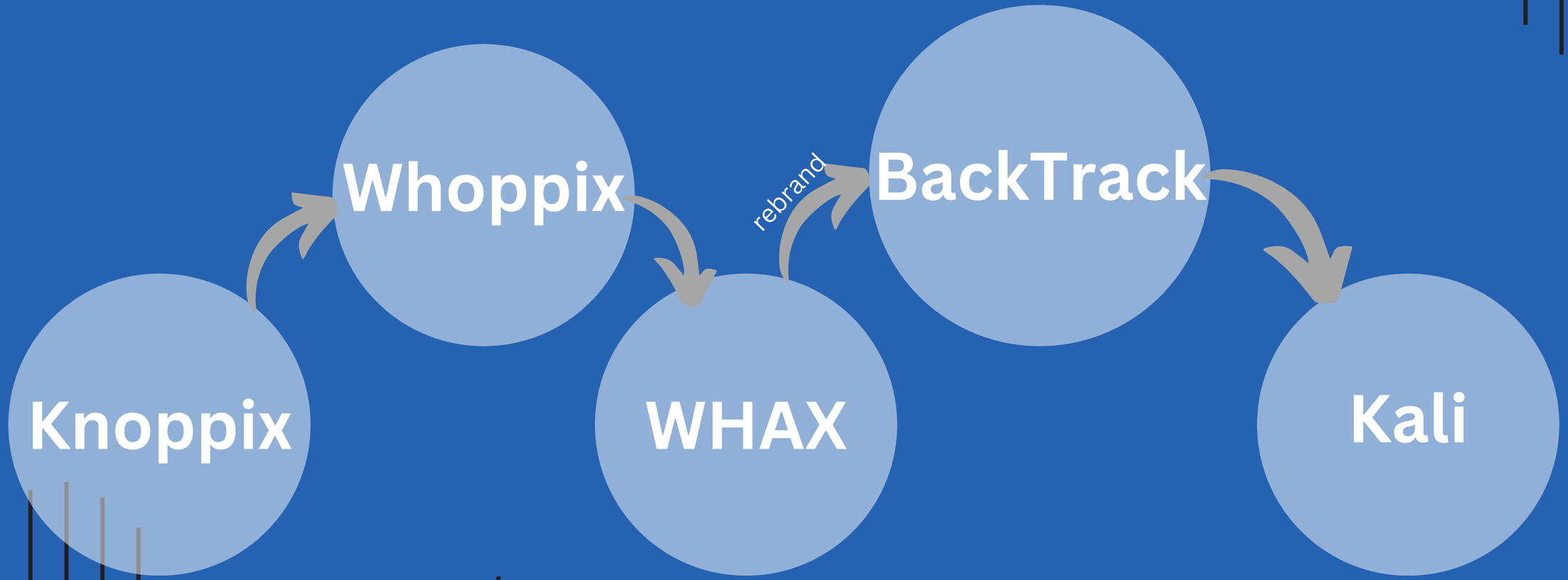
open-source distribúcia

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 zariadený fungujuce na ARM)

niektoré z nástrojov kali linux

nástroje na zhromažďovanie informácií

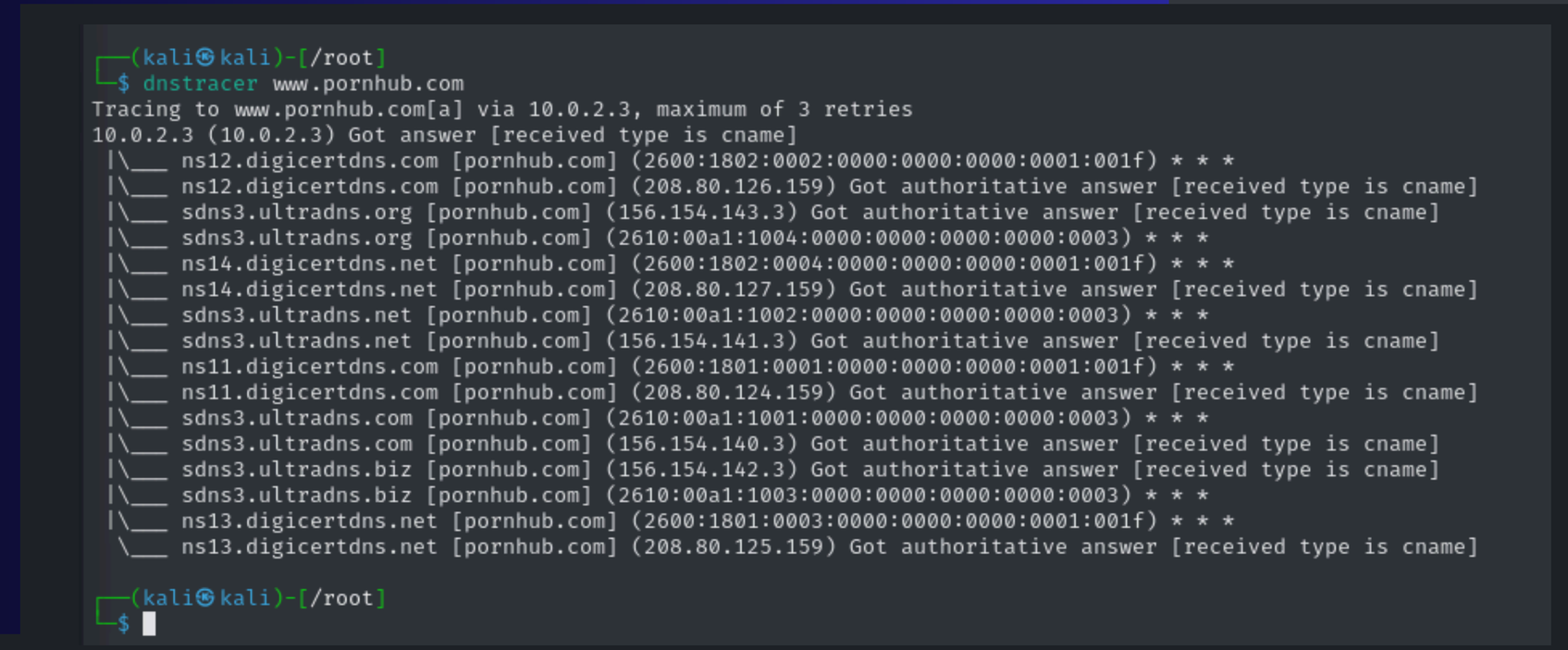
- dnsdict6
- dnsenum
- dnsmap
- dnsrecon
- dnsrevenum6
- dnstracer
- dnswalk
- fierce
- maltego
- nmap
- urlcrazy

```
┌──(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]
```

nmap

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

skenuje hostiteľa, snaží sa identifikovať nainštalované služby



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

                    ______
                   /      \
                  (  Woof! )
                   \  ____/
                   ,,
      .-.  -      _______                    )
     ()``; |=|___/_____)                  ) (_
    / ('          /|\                    ( |__|
(  /  )          / | \                  .)|__|
 \(_)_))        /  |  \                (  |__|
                                        . |__|
                                          |__|

                ~ 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

                    ______
                   /      \
                  (  Woof! )
                   \  ____/
                   ,,
      .-.  -      _______                    )
     ()``; |=|___/_____)                  ) (_
    / ('          /|\                    ( |__|
(  /  )          / | \                  .)|__|
 \(_)_))        /  |  \                (  |__|
                                        . |__|
                                          |__|

                ~ 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

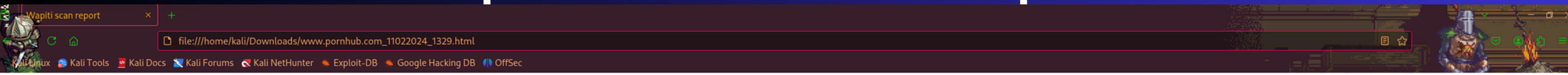
skenery zraniteľnosti webu

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

wapiti

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

odpoveď 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

webové aplikácie fuzzlers

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

zneužívanie databázy

- bbqsql
- sqlninja
- sqlsus

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