

5 Rarest Tools used in Linux :-

1. FLUXION
2. LYNIS
3. NIKTO
4. SKIPFISH
5. JOHN THE RIPPER

1. FLUXION



Fluxion is a Wi-Fi analyzer specializing in MITM WPA attacks and lets you scan wireless networks.

Pen testers use Fluxion to search for security flaws in corporate and personal networks. However, unlike similar Wi-Fi cracking tools, Fluxion does not launch time-consuming brute force cracking attempts.

Instead, Fluxion creates an MDK3 process that forces all users on the targeted network to lose authentication or deauthenticate. Once this is accomplished, the user is prompted to connect to a false access point, requiring entering the Wi-Fi password. Then, the program reports the password to the pen tester to gain access.

2. LYNIS

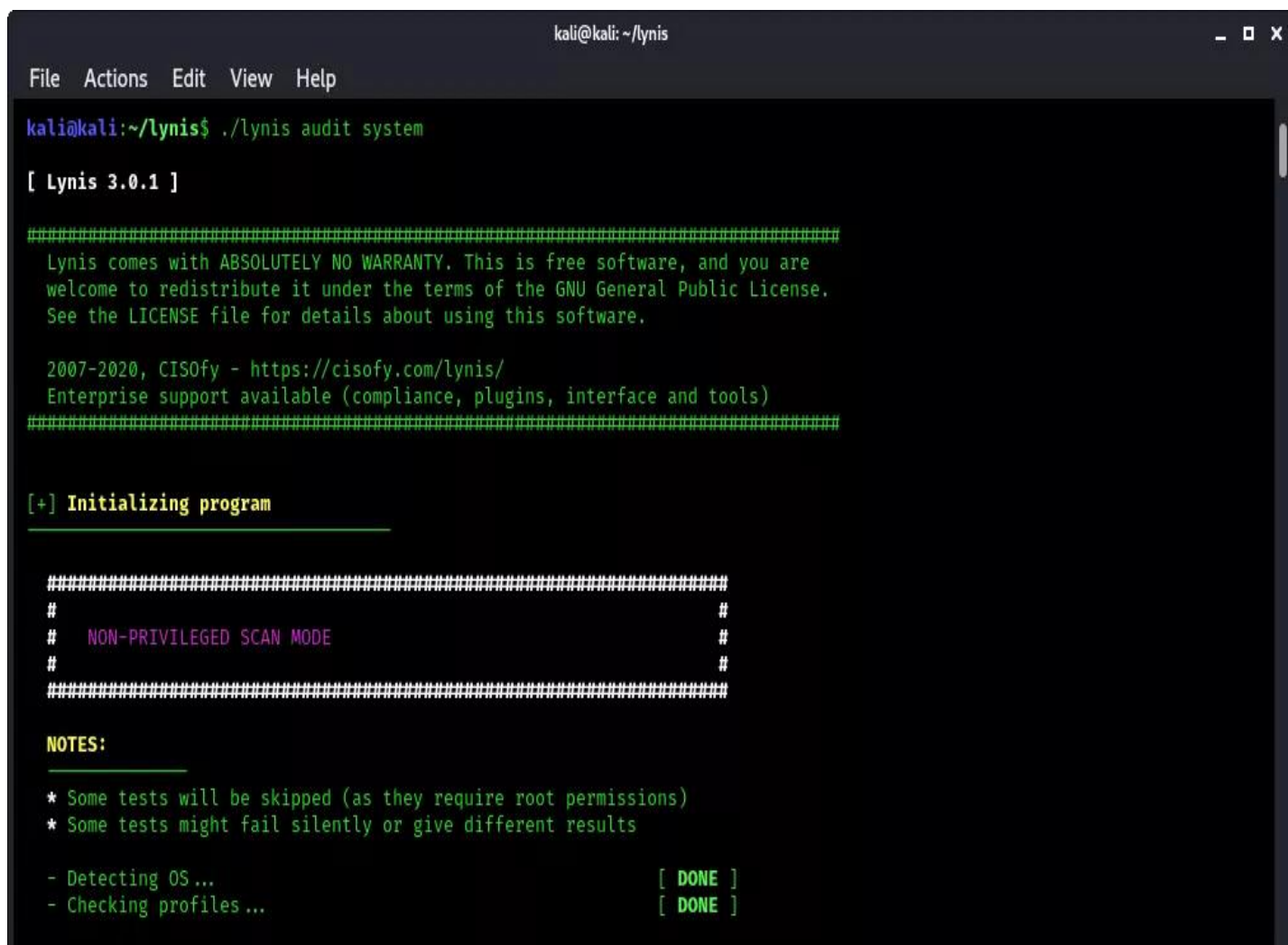
Lynis is most likely one of the most comprehensive tools available for cybersecurity compliance (e.g., PCI, HIPAA), system auditing, system hardening, and testing. In addition, thanks to its numerous capabilities, Lynis also functions as an effective platform for vulnerability scanning and penetration testing.

This Kali Linux tool's main features include:

Open source and free, with commercial support available. Simple installation from the Github repository.

It runs on multiple platforms (BSD, macOS, Linux, BSD, AIX, and more). It can run up to 300 security tests on the remote host.

Its output report is shared on-screen and features suggestions, warnings, and any critical security issues found on the machine.



```
kali@kali: ~/lynis
File Actions Edit View Help

kali@kali:~/lynis$ ./lynis audit system

[ Lynis 3.0.1 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2020, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program

#####
#
#  NON-PRIVILEGED SCAN MODE
#
#####

NOTES:
- Some tests will be skipped (as they require root permissions)
- Some tests might fail silently or give different results

- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
```

3. NIKTO

Nikto enables ethical hackers and pen testers to conduct a complete web server scan to discover security vulnerabilities and related flaws. This scan collects results by detecting default file names, insecure file and app patterns, outdated server software, and server and software misconfigurations.

Written in Perl, Nikto complements OpenVAS and other vulnerability scanners. In addition, it features support for host-based authentication, proxies, SSL encryption, and more.

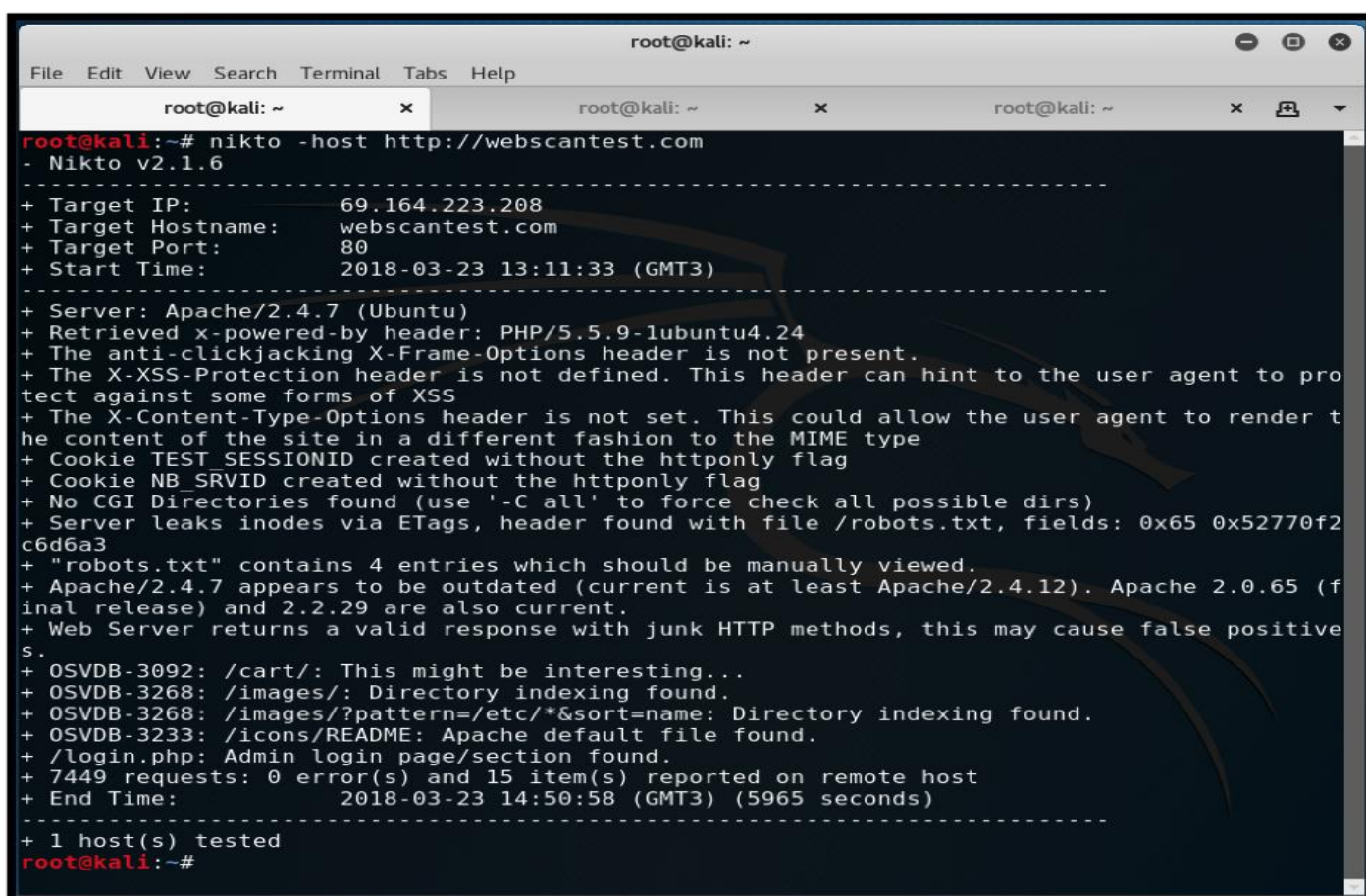
Nikto's primary features include:

- Scanning multiple ports on a server.
- Providing IDS evasion techniques.

- Outputting results into TXT, XML, HTML, NBE or CSV.
- Apache and cgiwrap username enumeration.

- Identifying installed software via headers, files, and favicons.
- Scanning specified CGI directories.

- Using custom configuration files.



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x  
root@kali:~# nikto -host http://webscantest.com  
- Nikto v2.1.6  
-----  
+ Target IP: 69.164.223.208  
+ Target Hostname: webscantest.com  
+ Target Port: 80  
+ Start Time: 2018-03-23 13:11:33 (GMT3)  
-----  
+ Server: Apache/2.4.7 (Ubuntu)  
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Cookie TEST_SESSIONID created without the httponly flag  
+ Cookie NB_SRVID created without the httponly flag  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2c6d6a3  
+ "robots.txt" contains 4 entries which should be manually viewed.  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.  
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.  
+ OSVDB-3092: /cart/: This might be interesting...  
+ OSVDB-3268: /images/: Directory indexing found.  
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ /login.php: Admin login page/section found.  
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2018-03-23 14:50:58 (GMT3) (5965 seconds)  
-----  
+ 1 host(s) tested  
root@kali:~#
```

4. SKIPFISH

```
root@kali:~# skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [ options ... ] -W wordlist -o output_dir start_url [ start_url2 ... ]

Authentication and access options:

-A user:pass      - use specified HTTP authentication credentials
-F host=IP        - pretend that 'host' resolves to 'IP'
-C name=val       - append a custom cookie to all requests
-H name=val       - append a custom HTTP header to all requests
-b (i|f|p)        - use headers consistent with MSIE / Firefox / iPhone
-N               - do not accept any new cookies
--auth-form url   - form authentication URL
--auth-user user  - form authentication user
--auth-pass pass  - form authentication password
--auth-verify-url - URL for in-session detection

Crawl scope options:

-d max_depth      - maximum crawl tree depth (16)
-c max_child      - maximum children to index per node (512)
-x max_desc       - maximum descendants to index per branch (8192)
-r r_limit        - max total number of requests to send (100000000)
-p crawl%         - node and link crawl probability (100%)
-q hex           - repeat probabilistic scan with given seed
-I string         - only follow URLs matching 'string'
-X string         - exclude URLs matching 'string'
-K string         - do not fuzz parameters named 'string'
-D domain        - crawl cross-site links to another domain
-B domain        - trust, but do not crawl, another domain
-Z               - do not descend into 5xx locations
-O               - do not submit any forms
-P               - do not parse HTML, etc, to find new links
```

Skipfish is a Kali Linux tool like WPScan, but instead of only focusing on WordPress, Skipfish scans many web applications. Skipfish acts as an effective auditing tool for crawling web-based data, giving pen testers a quick insight into how insecure any app is.

Skipfish performs recursive crawl and dictionary-based tests over all URLs, using its recon capabilities. The crawl creates a digital map of security checks and their results.

Noteworthy Skipfish features include:

- Automated learning capabilities.
- Differential security checks.

- Easy to use.

- A low false positive ratio.

- The ability to run high-speed security checks, with over 200 requests per second.

5. JOHN THE RIPPER

John the Ripper gets points for a creative name. This hacker's resource is a multi-platform cryptography testing tool that works equally well on Linux, Windows, macOS, and Unix. It enables system administrators and security penetration testers to test the strength of any system password by launching brute force attacks. Additionally, John the Ripper can be used to test encryptions like DES, SHA-1, and many others.

Its ability to change password decryption methods is set automatically and contingent on the detected algorithms.

John the Ripper's advantages :

- BruteForce and Dictionary attacks

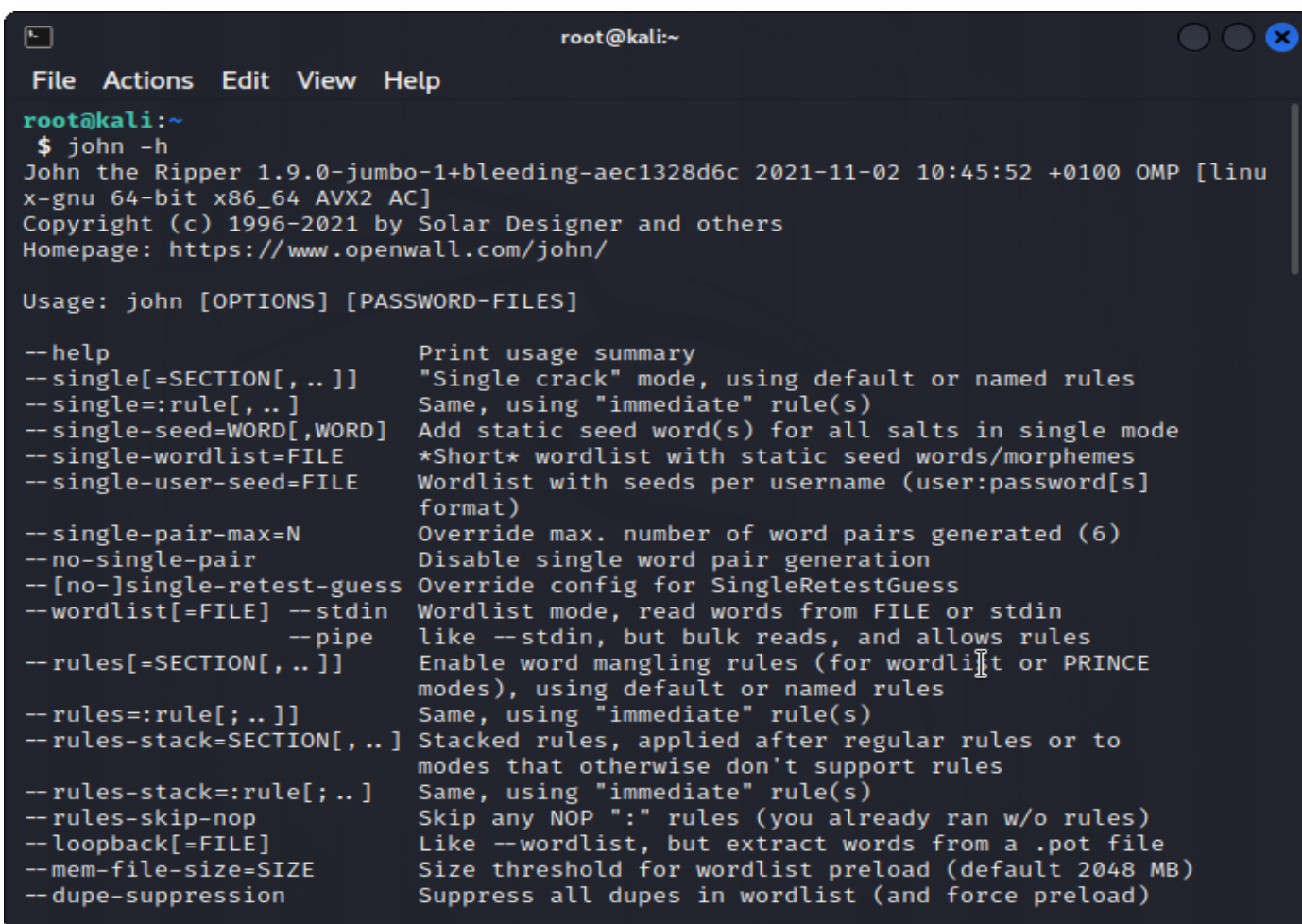
- Compatibility with most operating systems and CPU architectures

- Running automatically by using crons

- Allowing Pause and Resume options for any scan

- It lets hackers define custom letters while building dictionary attack lists

- It allows brute force customization rules

A screenshot of a terminal window titled 'root@kali:~'. The window shows the output of the command 'john -h'. The output includes the version 'John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c', the date and time '2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]', the copyright 'Copyright (c) 1996-2021 by Solar Designer and others', and the homepage 'Homepage: https://www.openwall.com/john/'. Below this is the usage line 'Usage: john [OPTIONS] [PASSWORD-FILES]' and a list of options with their descriptions. The options are: --help (Print usage summary), --single[=SECTION[, ..]] (Single crack mode), --single=:rule[, ..]] (Same, using immediate rule(s)), --single-seed=WORD[,WORD] (Add static seed word(s)), --single-wordlist=FILE (Short wordlist with static seed words), --single-user-seed=FILE (Wordlist with seeds per username), --single-pair-max=N (Override max. number of word pairs), --no-single-pair (Disable single word pair generation), --[no-]single-retest-guess (Override config for SingleRetestGuess), --wordlist[=FILE] --stdin (Wordlist mode, read words from FILE or stdin), --pipe (like --stdin, but bulk reads), --rules[=SECTION[, ..]] (Enable word mangling rules), --rules=:rule[; ..]] (Same, using immediate rule(s)), --rules-stack=SECTION[, ..]] (Stacked rules), --rules-stack=:rule[; ..]] (Same, using immediate rule(s)), --rules-skip-nop (Skip any NOP rules), --loopback[=FILE] (Like --wordlist, but extract words from a .pot file), --mem-file-size=SIZE (Size threshold for wordlist preload), and --dupe-suppression (Suppress all dupes in wordlist).