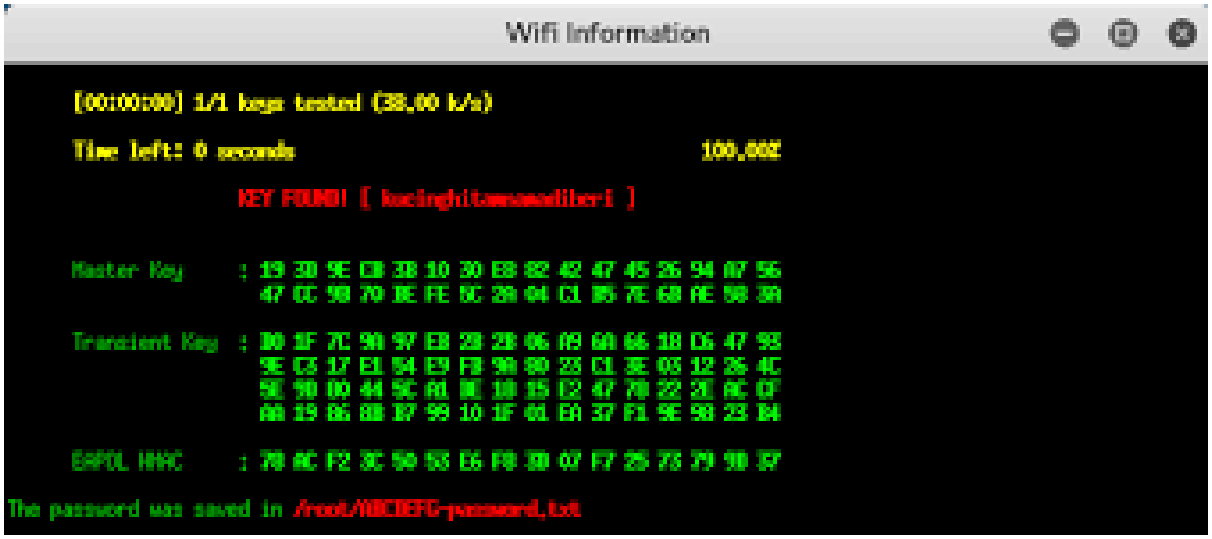
-> Exploring some Kali tools :-

- 1.) Fluxion :

- Description : It 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.

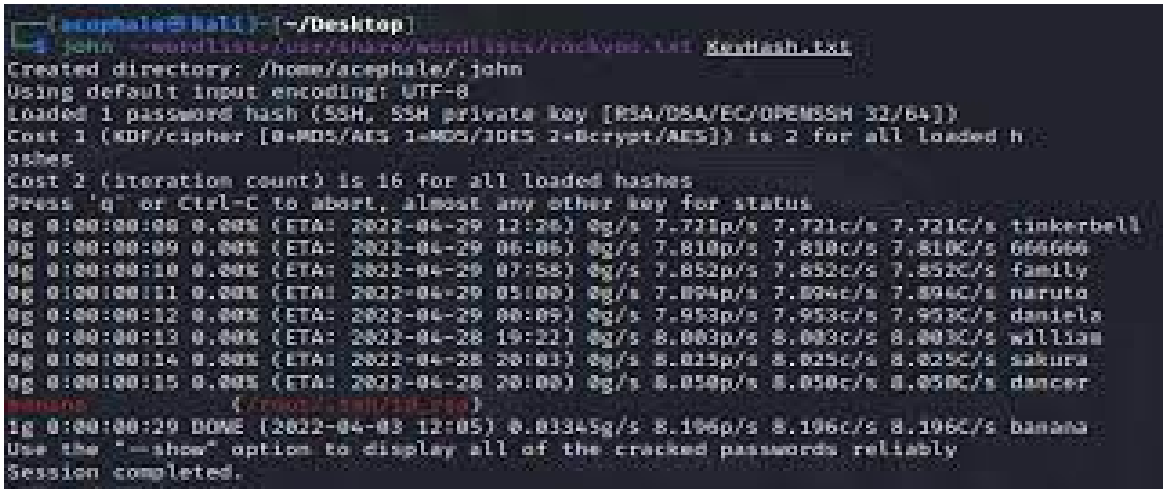
- Image :



- 2.) John the Ripper :

- Description : 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 is a free tool, licensed and distributed under the GPL license, and ideal for anyone who wants to test their organization's password security.

- Image :



- John the Ripper’s chief advantages include:
    1.) Brute force testing and dictionary attacks.
    2.) Compatibility with most operating systems and CPU architectures.
    3.) Running automatically by using crons.
    4.) Allowing Pause and Resume options for any scan.
    5.) It lets hackers define custom letters while building dictionary attack lists.
    6.) It allows brute force customization rules.

- 3.) Lynis :

- Description : It is most likely one of the most comprehensive tools available for cybersecurity compliance (e.g., PCI, HIPAA, SOx), 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.

- Image :

- This Kali Linux tool’s main features include:
    1.) Open source and free, with commercial support available.
    2.) Simple installation from the Github repository.
    3.) It runs on multiple platforms (BSD, macOS, Linux, BSD, AIX, and more).
    4.) It can run up to 300 security tests on the remote host.
    5.) Its output report is shared on-screen and features suggestions, warnings, and any critical security issues found on the machine.

- 4.) Metasploit Framework :
-
- Description : It is a Ruby-based platform used by ethical hackers to develop, test, and execute exploits against remote hosts. Metasploit includes a complete collection of security tools intended for penetration testing, plus a powerful terminal-based console known as msfconsole, which lets you find targets, exploit security flaws, launch scans, and collect all relevant available data.Available for Windows and Linux, MSF is most likely one of the most potent security auditing Kali Linux tools freely available for cybersecurity professionals.

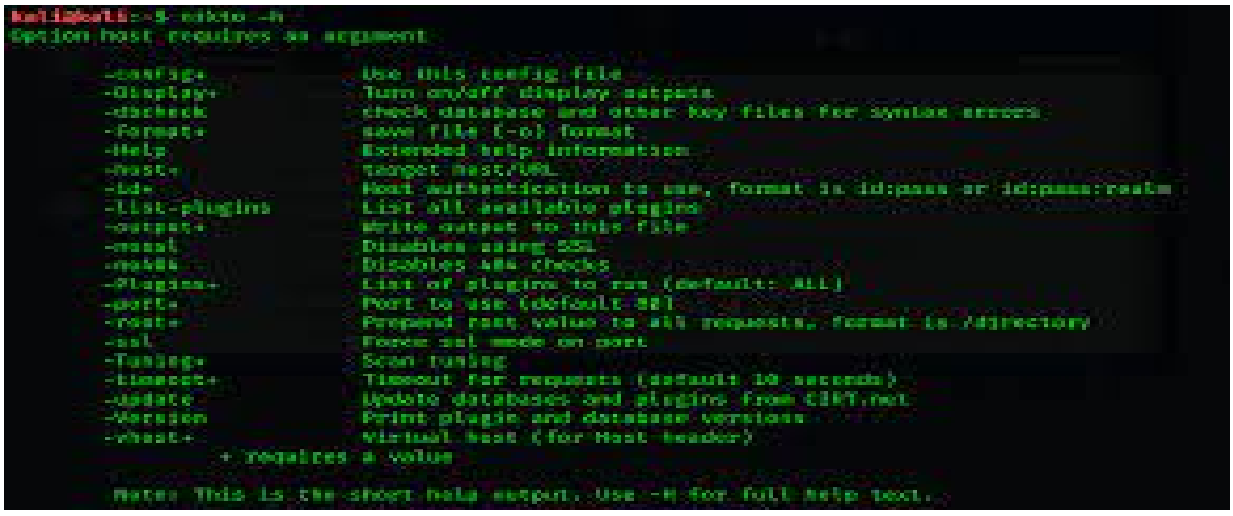
- Image :

- Metasploit Framework’s features include:

1.) Network enumeration and discovery.
2.) Evading detection on remote hosts.
3.) Exploiting development and execution.
4.) Scanning remote targets.
5.) Exploiting vulnerabilities and collecting valuable data.

- 5.) Nikto :
- Description : It 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.

- Image :

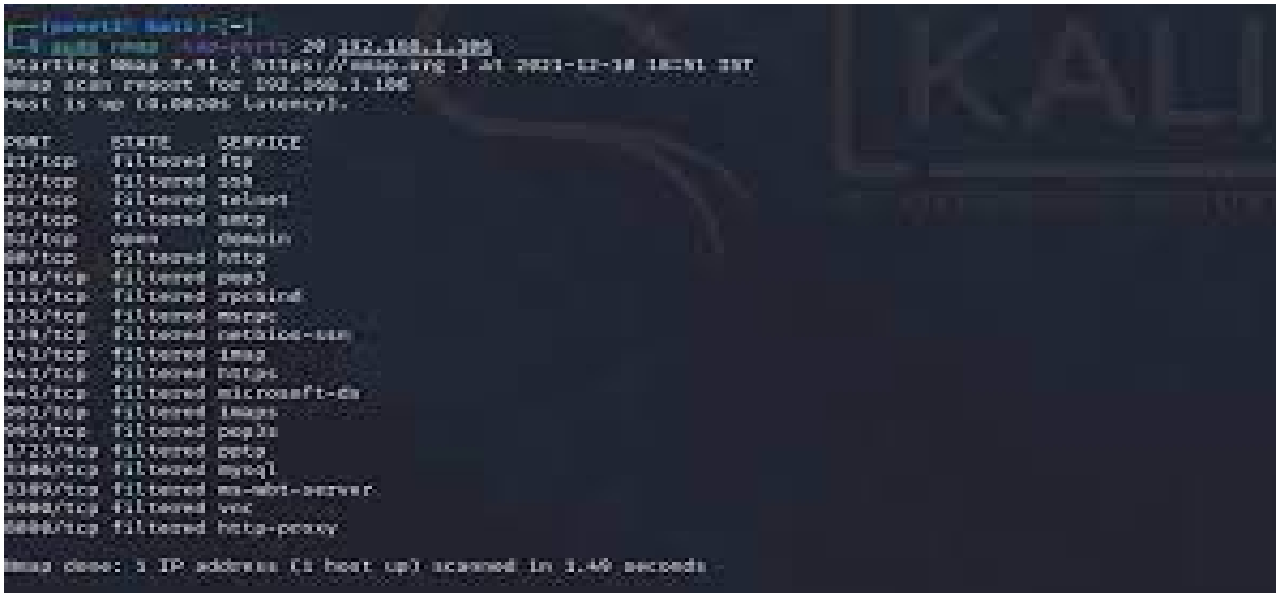


- Nikto’s primary features include:
    1.) Scanning multiple ports on a server.
    2.) Providing IDS evasion techniques.
    3.) Outputting results into TXT, XML, HTML, NBE or CSV.
    4.) Apache and cgiwrap username enumeration.
    5.) Identifying installed software via headers, files, and favicons.
    6.) Scanning specified CGI directories.
    7.) Using custom configuration files.

- 6.) Nmap :

- Description : It is the most well-known network mapper tool in IT circles. It lets you discover active hosts within any network and gain additional information related to penetration testing, such as existing open ports.

- Image :

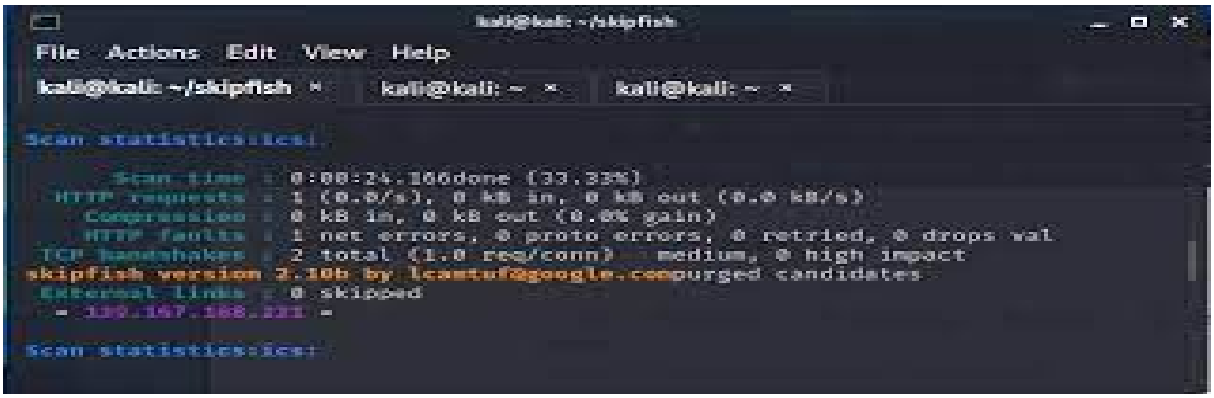


- Nmap main features include:
    1.) Host discovery, which identifies hosts in any network.
    2.) Port scanning lets you enumerate open ports on either a local or remote host.
    3.) OS detection helps gather operating system and hardware info about any connected device.
    4.) App version detection lets you determine the application name and version numbers.
    5.) Scriptable interaction extends the Nmap default capabilities by using the Nmap Scripting Engine (or NSE).

- 7.) Skipfish :

- Description : It 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.

- Image :



- Noteworthy Skipfish features include:
    1.) Automated learning capabilities.
    2.) Differential security checks.
    3.) Easy to use.
    4.) A low false positive ratio.
    5.) The ability to run high-speed security checks, with over 200 requests per second.