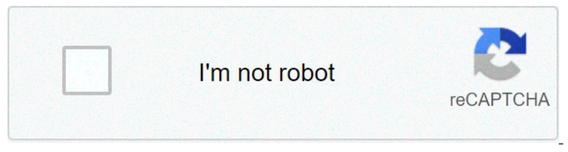

Continue

Pentesting with kali linux pdf

Aws pentesting with kali linux pdf. Practical guide to windows pentesting with kali linux. Pentesting with kali linux course. Active directory pentesting with kali linux. Pentesting with kali linux pdf. Aws pentesting with kali linux. Pentesting with kali linux tutorial. Pentesting with kali linux book.

Kali Linux is designed for penetration tests. Both the testha s starting point is tested white-box tests, black-box tests, or gray-box tests, there are always steps to follow during the execution of penetration tests with kali or other tools.step 1: reconnaissance Phasepror to an attack, the penetration tester should know the target environment and the characteristics of the system as much as possible. The most targeted information The penetration tester finds, the better the possibility of identifying the simplest and fastest way to succeed. Black-box testing requires more than white-box test reconnaissance, because testers do not get too much data. Scouting services can include tracks of the Internet to investigate the objectives, resource monitoring, staff monitoring, processes, etc., network information scanning (for example, IP addresses and system types) and social engineering public services such as helpdesk . Reconnaissance is the first step in the penetration test, both the penetration tester is known to confirm the destination system, or to find known intelligence. When reconnaissance, the destination environment must be defined according to the work area. Once the target is identified, a survey is performed to collect information about the destination, for example, that the doors for communication are used, in which the objective is hosted, such as services provides to the customer, and so on . These data can be used to develop a plan to see what the best way to get the desired results. The results of the reconnaissance process should include a list of all destination activities, which applications are associated with the activity, the services used and possible business owners. Kali Linux provides a category labeled a gatheringÃ ¢ information, which is a reconception resource. Tools include tools to investigate networks, data centers, wireless networks, and host systems. The following is a list of reconnaissance objectives: recognizing the objectives to define the use of applications and services by recognizing the type of system, confirming the available ports, confirming the services running, the information of social engineering, document Discovery.step 2 : Vulnerability Scanningafter confirms and investigating the goal through reconnaissance, the next step is to evaluate the target vulnerability. At this point, the penetration tester should be sufficiently informed about the target so that you can choose how to analyze the possible vulnerabilities or vulnerabilities. As the proverb says, there is no right to speak without investigations. The field of application of the test vulnerability can include the web application how to perform, such as services, leads what communication, and so on. The computer security audit often comes at this stage of the destination evaluation process. Scouting for information able to improve the accuracy of identifying potential vulnerabilities, reduce the time required for services and help avoid existing target safety. For example, performing a generic vulnerability scanner for a web application server could potentially warn the owner of the good, generating only general details on the system and the application. Depending on the data acquired during the reconnaissance phase, scanning the server for specific vulnerabilities can be more difficult for the network owner, providing an easy-to-use vulnerability and time for its implementation. The vulnerability of the evaluation objectives can be automated manually or through tools. There is a set of tools in Kali Linux called Vulnerability Analysis. The functionality of these tools range from of network devices for database aspects. The following list shows the evaluation objectives: to evaluate the vulnerability of the destination system; Priority of the vulnerable system; mapping of the vulnerable system to the owner of savings; and discovered recording problem.step 3: Exploitation this step to use the gaps found to check if these vulnerabilities are true, and verify what is access or o It can be. Exploit vulnerabilitates to separate penetration test services from passive services such as evaluation and auditing of vulnerability. Exploits of vulnerability and all subsequent steps can be obtained legitimately without the authorization of the owner of the target system. The success of this passage depends mainly on the previous work. Most exploits developed for specific vulnerabilities and can cause unpredictable results if executed incorrectly. The best approach is to identify some vulnerabilities and therefore develop an attack strategy against vulnerabilities that are more vulnerable to exploitation. The process of exploiting the vulnerability of the target system can be manual or automated, based on the final goal. There are cases in which the SQL injection is performed to obtain administrative access to the web application or, through social engineering, to allow the service service staff to provide administrator access credentials. Kali Linux offers a series of specific exploits tools called exploitation tools to exploit targeted vulnerabilities ranging from exploiting specific service vulnerabilities to social engineering packages. The following are some of the Exploit objectives: exploiting vulnerabilities; Get access; capture unauthorized data; active implementation social engineering; attack other systems or applications; and registration of discoveries. 4: PrivilegeÃ ¢ EscalatoAccess The objectives do not guarantee that infiltration tasks can be completed. In many cases, the use of a vulnerable system can request access to limited data and resources. The attackers must be privileged to access critical data (sensitive data, critical infrastructures). The elevation of the privilege can include the recognition and breakage of passwords, user accounts, IT space not fired and so on. For example, an attacker could implement the limited user access, confirm a shadow file that contains the administrator's login credentials, get password for the administrator via password cracking and access the internal application via access of the administrator. Toolkit of attacks and vulnerability of the Kali Linux password provides a number of tools to help you get an elevation of the privilege. Because most of these tools include methods to get initial access and elevation of the privilege, these tools are grouped based on the tool set. The following lists the Escalation objectives of the privilege: obtain the highest privileges to access the system and the network; reveal other information about the user account; access privileged access to other systems; and recording of the discoveries.sep 5: Keeping access to access is to keep access by establishing other points of entry to the target and, if possible, to cover the penetration test. The penetration process can trigger a defense mechanism, which eventually contributes to ensuring that the security of the penetration tester when accessing the network. The best approach is to establish other means of access to the target as a guarantee that the main path is closed. Alternative access methods can be backdoors, new administrator accounts, encrypted channels, new network access channels and so on. Another important aspect of establishing a support point in the destination system is the removal of penetration tests. This can make the detection of attack more difficult, and therefore can reduce the response to the defense of security. Compensation tests include the elimination of user logs, mask existing access channels The cancellation of corruption traces (such as error messages caused by the infiltration process). Kali Linux includes a directory called Ã ¢ â,¬ Å "Maintaining AccessÃ ¢ â,¬, whose goal is to maintain a support point on the destination system. To create various forms of backdoors in the destination system, tools are needed. The objective of establishing a support point on the destination system is the following: establishing more access points on the destination network; Removal of evidence that access was granted; repair the affected system; Encryption and other means of vehicles hide the communication method; Record the findings.sep 6: ReportingReporting phase is the last phase in the penetration test methodology. The signaling phase will be verified with the other three phases or will happen after the attack phase. This reporting phase is a very vital phase and this report is the management and the technical aspects, provide detailed information on all the conclusions, the figures with correct graphs. The penetration tester will provide an adequate presentation of vulnerabilities and its impact on the business of the target organization. The final document will be described and will provide a technical description of the vulnerability. Penetration tester should meet the customer's requirement in documents also the document should be detailed and that will show the successful penetration tester. One of Kali's best things is the fact that it does not require you to install the operating system on your hard drive Ã ¢ â,¬ "uses a live image that can be loaded into the RAM memory to test your safety capabilities with The more than 600 ethical hacking tools that provides. Includes numerous security-hacker tools for collecting information, vulnerability analysis, wireless attacks, web applications, exploitation tools, stress tests, tools Forensics, Skding and spoofing, password cracking, reverse engineering, hardware and much more. We have previously explored the first 20 OSINT tools available, and today we pass through the list of Kali Linux software at the top. Start! Kali Linux USA What are called Ã ¢ â,¬ Å "Kali Linux MetapackagesÃ ¢ â,¬" These metapackages allow you to install series of tools, instead of requiring to install all Kali Linux D tools They are positioned in the repo. For example, if you continue to use only Kali Linux tools for wireless security assessment, you can simply generate an ISO kali image and include only Kali-Linux-Wireless metapackage. For the purposes of this post, refer to the best Kali Linux tools in general, regardless of metapackages to which they belong. For reference facilities, we divide the most used Kali Linux software into five distinct categories: information collection, vulnerability scan, wireless analysis tools, password crackers, exploitation tools and stress tests. 1. Nmap nmap is the world's most famous network mapper tool. It allows you to discover hosted hosts within any network and acquire other information (as open doors) related to penetration tests. Main features: Discovery Host: Useful for identifying hosts in any network port scanning: lists the open ports on the detection of the local or remote host operating system: useful for recovering the operating system and hardware information on any version detection App for connected devices: allows you to determine application name and number of scriptable interaction version: extends NMAP default capabilities using NMAP Scripting Engine (NSE) [SecurityTrails @ Kali Root] $ nmap - Using DelHelp: nmap [Type of scan / i] [Options] {Target specification} Specification Target: Pass Hostnames, IP addresses, networks, etc. Ex: scanMe.nmap.org, microsoft.com/29, 192.168.0.1; 10.0.0-255.1-254 -The : Insert from the list of hosts / networks -Ir : Choose random targets - Excluding : Host / Networks Exclusion --Excludefile : Exclusion List from Host File Discovery: -SL: Scan List - just list the goals to scan -sn: ping scan - Disable the port door: it treats all hosts like online - Skip Host Discovery -PS / PA / PU / PY [Portlist]: TCP Syn / Ack, UDP or SCTP For ports supplied -pe / pp / pm: ICMP echo, timestamp and netmask request the detection probes -po [protocol list]: IP ping -n / -r protocol: never run the dns / resolution resolution [default: a Times] - Server-server : Specify custom DNS servers - SYSTEM-DNS: Use the DNS resolver of the operating system - TRACE HOP PATH for each host ready to trigger the Nmap power? Take a look at our list of the first 15 15 Commands. 2. Lynis Lynis is probably one of the most complete tools available for cybersecurity compliance (eg PCI, HIPAA, SOX), test, hardening system and system control. This is why it is included in this list of Kali Linux tools. Given its immense capacity, Lyis also serves as a large vulnerability scanner and penetration test platform. Its features and its main features include: Open Source Free - With commercial support available Easy Installation from Github Repository Run more platforms (BSD, MacOS, Linux, BSD, AIX and others) Runs up to +300 Safety tests on the report Remote Host Output is shared on the screen, including suggestions, warnings and security problems found on the machine 3. Fierce Fierce is a great tool for network mapping and scanning the door. It can be used to discover the un contiguous IP space and host names through networks. It is similar to Nmap and UnicornScan, but unlike those, fierce is also used for specific corporate networks. Once the penetration tester has defined the destination network, FIARE will perform different tests than the selected domains to retrieve valuable information that can be used for subsequent analysis and exploitation. Its features include: Capacity to modify the DNS server for inverse searches and internal interior and external IP intervals Scan the IP range and entire class C The functionalities of the scan registers in a file system system System Discovery and Transfer ATTACK ATTAK file Functionality with integrated or personalized text list. OpenVas Openvas (open vulnerability system) was developed by the team responsible for the famous Nessus vulnerability scanner. Licensed under the GLP license, it is the free software that anyone can use to explore local or remote network vulnerabilities. This security tool allows you to write and integrate your safety plugins to the OpenVas platform - even if the current motor is supplied with more than 50K NVTS (network vulnerability test) that can literally scan everything you imagine in terms of vulnerabilities Safety. Main features: Simultaneousy Host Discovery Network Mapper and Port Scanner Support for the OpenVas Transfer Protocol fully integrated with SQL databases as SQLite scheduled for daily or weekly scans of results exports to XML, HTML, latex file formats to interrupt , Pause and resume full support scans for Linux and Windows 5. Nikto written in Perl and included in Kali Linux, Nikto IWorks as an openvas complement and other vulnerability scanners. Nikto allows penetration testers and ethical hackers to scan a complete web server to discover safety defects and vulnerabilities. This security scanning collects the results by detecting insecure files and app patterns, obsolete server software and default file names as well as server and server and software servers. Includes support for proxies, host-based authentication, SSL encryption and much more. The main features include: scans multiple ports on an IDS Techniques Evasion server outputs results in TXT, XML, HTML, NBE or CSV. The Apache and CGIwrap username enumeration identifies the software installed by headers, Favicon and specified CGI directory scans files use custom debug and verbose output configuration files. 6. WPSCAN WPSCAN is recommended to check the security of WordPress installation. Using WPSCAN you can check if your WordPress set-up is vulnerable to certain types of attacks, or if you expose too many In the main files, plugins or theme. This WordPress security tool also allows you to find weak passwords for all registered users and even perform a brute force attack against it to see which can be cracked. WPSCAN receives frequent updates from the WordPulndb.com WordPress vulnerability database, which makes it excellent updated WP security software. What can you do with WPSCAN? Non-interabered security scans WP NEGGIORNO Enumeration WP BruteForce Attack & weak Password cracking WP plugins plugins vulnerability enumeration WordPress SECURITY Are you interested in Wordpress Security? Check out our blog post to ask exactly that: WordPress is safe? 7. Skipfish Another worthy addition to our list of Kali Linux tools is Skipfish. This tool is similar to WPScan, but rather than just focusing on Wordpress, Skipfish scan a large amount of Web applications, serving as an excellent control tool for scanning web-based data, and provides quick information on as it is unsafe for your app. With its ability to return, run a recursive crawl and dictionary-based testing on all of your URL, creating a digital map of security checks along with the results for each of them. The considerable Skipfish features include: high-speed security controls (200+ requests per second) Easy to use learning Capacity automatable Low false positive ratio of differential safety Controls 8. CMSMAP Unlike the WPScan, CMSMAP aims to be a centralized solution not just one, but the top four of the most popular CMS in terms of vulnerability detection. CMSMAP is an open source project written in Python that helps automate the scanning and detection process of vulnerability in Wordpress, Joomla, Drupal and Moodle. This tool is not only useful for detecting security defects in these four popular CMS but also to perform brute force attacks and launch actual exploits once a vulnerability was found. The main features include: supports multiple virus scanning the ability to set a custom user support and header support for SSL encryption. The verbose mode for debugging purposes saves the output to a text file. 9. Fluxion Fluxion is a WiFi analyzer specialized in WPA MITM attacks. It allows you to scan for wireless networks, looking for security flaws in business and personal networks. Unlike other WiFi Cracking tools, the flow does not cast any attempt to brute force cracking that usually takes a long time. Instead, it generates a MDK3 process that forces all users connected to the target to deautanti network. When finished, the user is prompted to connect to a fake access point, where it will enter the WiFi password. So the program will warn the password for you, so you can access. 10. Aircrack-ng Aircrack-ng is a wireless security software suite. It consists of a network packet analyzer, a network WEP crackers and WPA / WPA2-PSK with another set of wireless monitoring tools. Here are the most popular tools included in the suite Aircrack-Ng: airmon-NG: converts your wireless card into a wireless card in a promiscuous mode airmon-NG: Captures the desired specific packages, and T is particularly useful in deciphering passwords NG: used to decrypt passwords Ã ¢ ¬ "able to use statistical techniques to crack wEP and WPA and WPA2 dictionaries for having captured the WPA handshake Aireplay-NG: it can be used to generate or accelerate traffic at a point access airdecap-NG: decrypts wireless Traffic once the key is decrypted key features: Support for WEP, WPA / WPA2-PSK Passwords Fast WEP and WPA Password Sniffer DECRYPTION PACKAGE injector and injector Ability to create an automated virtual tunnel WEP key password Recovery password list Management [SecurityTrails @ Kali Root] $ aircrack-ng aircrack-NG 1.2 RC4 - (c) 2006-2015 Thomas D'Otreppe http: //www.aircrack-ng .org Use: Aircrack-ng [options] Common options: -a : Force Attack Mode (1 / WEP, 2 / WPA-PSK) -e : target selection: network identifier -b : target Selection: Mac -P of the access : # of CPU (Default: All CPUs) -Q: Enable the silent mode (no status output) -C : JOIN THE APS Specified in a virtual file : Writing button for file 11. Kismet wireless wireless Kismet wireless It is a free multi-platform wireless LAN analyzer, sniffer and ID (intrusion detection system). It is compatible with almost any type of wireless card. Use it in Sniffing mode allows you to work with wireless networks like 802.11a, 802.11b, 802.11g and 802.11n. Kismet wireless works natively in Windows, Linux and BSD BSD operating systems NETBSD, OpenBSD and MacOS). Main features: Capacity to run in passive easy detection mode of wireless clients and access points The wireless intrusion detection system scans wireless encryption levels for a specific AP supports hopping network recording 12. Wireshark Wireshark is An open source multi-platform network analyzer that runs Linux, OS X, BSD and Windows. It is particularly useful for knowing what is happening within your network, which represents its widespread use in governmental, corporate and educational industries. It works similarly to TCPDump, but Wireshark adds an excellent graphical interface that allows you to filter, organize and sort the acquired data to require less time to analyze. A text-based version, called Tshark, is comparable in terms of functionality. The main features include: GUI-friendly interface package Catch and offline analysis Complete protocol inspection GZIP compression and decompression on the VoIP sheet VoIP analysis Set support for IPsec, ISAKMP, Kerberos, SNMPV3, SSL / TLS, WEP and Wpa / wpa2 file formats such as tcpdump (libpcap), pcap ng, catapult dct2000, cisco secure iplog id and many others 13. john the ripper john the ripper is a multi-platform encryption test tool that works on unix, linux, windows And Macos. It allows system administrators and security penetration testers to start brute force attacks to test the strength of any system password. It can be used to test encryptions like DES, SHA-1 and many others. Your capacity to change the password's decryption methods are set automatically, depending on the algorithm detected. With license and distributed under the LPG license, it is a free tool available for anyone who wants to test their password security. The main features include: Dictionary attacks and brute strength tests compatible with most operating systems and CPU architectures can be performed automatically using the pause options of the chroniups and resume options for any scan allows you to define custom letters While the buildings of the attack lists allow the rules of customization of the Bruta force 14. THC Hydra THC Hydra is a free licensed hacking tool with AGPL V3.0, widely used by those who need Brute Force Remote Authentication Services. Because it supports up to more than 50 protocols, it is one of the best tools to verify password security levels in any type of server environment. It also provides support for the most popular operating systems such as Windows, Linux, free BSD BSD, Solaris and OS X. Main features: Ultrafast password cracking speed goes on more operating systems Capacity to start the application based on Attack Attacks Parallel modules Force Brute Attacks allows you to add custom module support for multiple protocols such as CVS, FTP, HTTP, HTTPS, HTTP-Proxy, IMAP, IRC, LDP, MS-SQL, MySQL, etc. 15. FindMyhash written in Python, FindMyhash is a free open source tool helps Crack Password using free online services. It works with the following algorithms: MD4, MD5, Sha1, SHA225, SHA256, SHA384, SHA512, RMD160, GOST, WHIRLPOOL, LM, NTLM, MySQL, Cisco7, Juniper, LDAP_MD5 and LDAP_SHA1. It also supports multi-thread analysis for rapid speed and algorithm recognition from the hash value. The main features include: empty hash recognition reads entry from a text file capacity to escape special single or multiple hash cracks. Search for your password hash on Google Pause and Resume Options Save results a file. 16. RainbowCrack RainbowCrackCrack is a password cracking tool available for Windows and Linux operating systems. Unlike other password cracking tools, RainbowCrack uses a complicated-memory-memory-memory algorithm for crack hash along with large pre-calculated tables Ã ¢ â,¬ Å "Rainbow" that help reduce password cracking time . The functionality include: interface available with regenal and gui-friendly works well with multi-core processors generation of the generation table, sorting, conversion and search for GPU acceleration (NVIDIA CUDA and AMD OpenCL) supports the rainbow table of any algorithm hash hash Charset. Supports the Rainbow table in the RAW file format (.rt) and the compact file format (.tc). Metasploit Framework is a ruby-based platform used to develop, test and execute Exploits on remote hosts. It includes a complete collection of security tools used for the penetration test, along with a powerful console based on the terminal - called MSFConsole Ã ¢ â,¬ "that allows you to find goals, launch scans, exploit safety defects and collect all I Available data. Available for Linux and Windows, MSF is probably one of the most powerful security control tools available for free for the InfoSec market. What can you do with Metasploit Framework? Network enumeration and discovery detection on remote hosts exploit The development and execution of the work with the remote goals of MFSconsole Scan scan exploit vulnerabilities and collect valuable data 18. Toolkit of social engineering (known as set) is a Python Open Source-based penetration test picture that will help you launch social-engineering attacks in no time weather. Have you ever wondered how to hack social network accounts? Well, set has the answer - it's essential for those interested in the field of social engineering. What kind of attack can I launch with sets? AP WIFI bindings: this type of attack redirects or intercepting packages from users who use our WiFi Network SMS and e-mail connections: here, the set will try to deceive and generate a false e-mail to get attacks Based on social credentials: it allows you to clone a web page so you can drive real users via DNS Spoofing or Phishing Attacks Attacks Creating Payloads (.exe) Loads: Set create a malicious .exe file, after executing, Comproprometer The user's system that shots on highlighted features include highlighted features: rapid penetration integration with third-party Phishing Attack Generator modules launches support for QRCode attacks for Powershell's attack carriers 19. Beef BEB Stands for the Browser exploitation framework, a powerful penetration test tool based on browser vulnerabilities and defects to take advantage of the HOS t. Unlike other Kali Cybersecurity tools, focuses on the side of the browser, including attacks against moving and desktop clients, allowing you to analyze the explosibility of any Mac and Linux system. You will be able to select specific modules in real time to check the security of the browser. Requirements for beef: OS: Mac OS X 10.5.0 or higher / contemporary Linux Ruby 2.3 or latest sqlite 3.x node.js 6 or more recent main features: web and console ui metasploit integration modular structure interprocess communication and exploitation gathering gathering And Intelligence Host and network reconnaissance capacity to detect browser plug-ins 20. Yersinia Yersinia is a security network tool that allows you to perform L2 attacks by exploiting safety defects in different network protocols. This tool can attach switches, routers, DHCP servers and many other protocols. Includes a GUI GTK Fancy, the NCURSES-based mode is able to read from a custom configuration file, supports debug mode and offers to save the results in a log file. Supported network protocols: 802.1q and 802.1x Wireless LANS Cisco Discovery Protocol (CDP) Dynamic host configuration protocol (DHCP) Dynamic Trunking Protocol (DTP) Inter-Switch Link Protocol (ISL) Hot Standby Protocol Protocol (STP) Protocol Tree (STP) VLAN TRUNKING PROTOCOL (VTP) 21. DHCPIG DHCPIG is a DHCP EXURING application that starts an advanced attack for All IPs active on the LAN. It also imports new users get IPS assigned to your computers. It works quite well that attacks Linux Lans and Windows 2003, 2008, etc. In fact, DHCPIG does not require any installation, as it is a tiny script; It only requires a library installed installed on your system and includes support for IPv4 and IPv6. What can you do with DHCPIG? Detect / Print DHCP Replies Detection / Print Requests ICMP Discover and create a network map of the IPS yourboursÃ ¢ â,¬ â "¢ â" ¢ request Possible IP addresses in a zone to create a cycle and send DHCP requests from different Mac addresses Explore your Neighbouts ¢ IP output and IP addresses and Mac address from the DHCP ARP server for all neighbors on that network Knock off on systems Windows 22. Funkload written in Python, funkload is a popular web-stress tool that works by emulating a completely functional web browser. It is very useful for testing web projects and see how well they react in terms of web server performance. Funkload allows complete performance tests to help identify possible bottlenecks within your web and web server applications, at the same time test the recoverability application time. Main features Funkload Include: The emulation of the real web browser (including / Post / Put / DELETE, DAV, Biscuit, REFERER SUPPORT GET, etc.) Advanced Test Row Complete Benchmarking Report in PDF, HTML, Rest, Org - Differential benchmark comparison between 2 customization test results using a full support file support for popular servers such as PHP, Python, Java 23. Slowhttptest Slowhttptest is one of the most popular web-stress applications used to launch DOS attacks against Any HTTP server. This type of security tool focuses on sending low bandwidth attacks to test response times for health and web server. It includes the statistics of all tests and allows you to perform more types of attacks such as: Apache interval header. Slow laws. Slow http post. Slow loris. The main features include: Saving HTML and CSV statistics output Level verbose setting file (0-4) Targeting custom number of connections Setting http connection speed (for seconds) Proxy Traffic Redirection 24. Inundator Inundator is a multi-tool Threaded protective protection ID Designed to be anonymous. Using Tor can flood intrusions detection systems (especially with snorts) cause false positives, which hide the real attack that takes place behind the scenes t. Using proxy socks can generate more than 1K positive false per minute during an attack. The main goal of Inundator is to keep your safety team dealing with false positives, while a real attack is happening. INDATOR Features and attributes: Multi-Threaded Socks features Full support Anonymization-Ready support of multiple tail-based targets 25. T50 T50 is another web stress test tool included with Linux Kali distribution. It can help you test how your websites, servers and networks react under high loading average during an attack. It is one of the few security tools capable of encapsulating protocols using GRE (Generic Routing Encapsulation), and supports up to 14 different protocols. The T50 package also allows you to send all the protocols in sequence using a single socket. T50 Features: DOS and DDOS connections Main simulator supported protocols include TCP, UDP, ICMP, IGMP, etc. up to 1,000,000 PPS of Syn Flood if you use network gigabits up to 120K PPS of Syn Flood if you use 100Mbps WEA VE network He said that before in our post as web software he is violated: a history of web vulnerability: internet a has no future without hacking ¢. Nowadays Kali Linux offers which are probably the best hackings and penetration tests ethical suite in the world. Thanks to their wide documentation, communities and tools, starting from the World InfoSec is not as difficult as it was 20 years ago; Nowadays you can find pre-built tools for almost everything you imagine. With the implementation of these Kali Linux tools, the company of It will have more possibilities to test and increase security of web applications and systems Ã ¢ by identifying safety failures before the bad guys do. We at SecurityTrails focused on creating a powerful security platform that includes domain automation lists, DNS forensic tools and IP exploration utilities as ever seen before. Our collection of information and intel data reconnection, combined with security distributions such as Kali, can make daily safety activities easier way than ever. never. never.