I'm not a robot

Hire Talent Drive performance and cyber resilience Retain Talent Select a Learning Journey IT Certifications University Bootcamps Workforce Development Military Benefits Hit button to validate captcha Do you need help in finding the best teacher matching your requirements? Post your requirement now Verified Free Demo Class : Available Average price : INR 400/hr Tutors available : 328 Class format : Online or Offline classes What is Kali Linux? Kali Linus is a Linux distribution that is Debian based. It is an OS that particularly caters to the likes of penetration testers and network analysts. The adjacent tools that come pre-installed with Kali actually convert it into an ethical hacking tool. Why do hackers use this? Ethical hacking has become very easy with this. Kali Linux is particularly known for testing-centric tools that are much more functional and easy to handle than other hacking tools. As all the tools are testing- centric helps the user stay safe and does not get involved with any legal charge. What are the tools that come along with Kali Linux? In Kali Linux software, there are pre-installed tools. Here are two of the most common and important tools. a. Aircrack-ng: These tools are used to assess any kind of WIFI network security. This focuses on the key region of WIFI security. This tool comprises a few sub-parts. These are Monitoring, Attacking, Testing, and Cracking. b. Nmap: Network Mapper, which is also known as Nmap, is an open and free utility source for security auditing and network discovery. This system has raw IP packets used to find out which hosts are active on the network. Apart from that, it also collects data of the services and what the hosts are offering, the name of the operating system can also be determined from it. Apart from these two, there are numerous tools of Kali that help to know more about the hosts. What is the fee for an Online Kali Linux Class? The course fee for an Online Kali Linux course depends on various factors. These factors can be a trainer's professional experience, education, location, and the number of live sessions given to the student. Find out the estimated course fee with the help of the UrbanPro tuition fee calculator. Which is the Best Online Kali Linux Class provider in India? There are many online Kali Linux class providers in India. To join the best institute, check out the reviews and ratings of coaching institutes available on UrbanPro to connect with experienced and reputed trainers. Kali Linux is already a known name in the IT industry. Offensive Security specifically funds this software. This information training company also maintains this software. Many, however, still tend to get confused about whether to use such software or not. Well, this software is handy, and many have found it beneficial. Here are some reasons people choose Kali Linux online courses. Anything that comes free is always good. There is no doubt that kali Linux is one such software that can help in many ways. So everybody always looks out for something which is readily available and for free. Most of the software available online is in English. Only a handful of the software is multi-lingual. Kali Linux provides various types of tools and is multi-lingual; people who do not understand English can try this software. So when someone is trying to learn this software, the trainer can choose the language the learner is comfortable with and use it. Following such a procedure helps the learners to get all the information quickly and learn it fast. This customisable option is thus a great help for the new learners. Yes, this software is programmed in such a way that it can be personalised. This is because the developers of this software have been very much liberal with developing it. The software can be programmed according to the requirement of the user. This gives ample opportunity to the users to try out their hands-on coding and do all they can do with the software to improve it and use it for their own benefits. Kali Linux online courses provide training to the learners to get used to the flexibility of the software. As Kali software is a member of the Linux family, it follows the open-source model. This development tree is displayed publicly on Git, and thus anyone can see it. Besides, the users can also tweak the code as they want to. The best reason for which Kali Linux is remembered is for the innumerable tools that anyone can get while using it. Generally, one user can get more than 600 tools that can be used for various types of testing. For security purposes, the tools available with Kali Linux are a great help. Many IT professionals until now have used it and found it helpful. So all of these are the best reasons to choose Kali Linux. However, learning Kali Linux could be a big challenge if someone is not aware of the course. Sometimes it becomes hard to get a proper idea about the system. So in such a situation, trusting a reputed educational platform would be the best thing to do. Browsing through the internet could help a lot. For the best result, it is thus recommended to join the Kali Linux courses online from a reputed platform like UrbanPro. To know more, check out the reviews and ratings of the Kali Linux courses online in India on UrbanPro LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (including professional and job ads) on and off LinkedIn. Learn more in our Cookie Policy.Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings. Register | Log in 0 ratings0% found this document useful (0 votes)4 viewsThe document provides a comprehensive list of Kali Linux commands for ethical hacking, categorized into sections such as system and network information, network scanning with Nmap, exploitatSaveSave Kali_Linux_Ethical_Hacking_Commands For Later0%0% found this document useful, undefinedThe most advanced Penetration Testing Distribution. Ever.Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Download Kali Linux Commands PDF for free. Learn 250+ best Kali Linux commands and increase your basic knowledge about Kali Penetration OS.Kali is the very first choice of all the people related to ethical hacking and penetration testing. There are dozens of reasons behind it. One reason is that Kali comes preloaded with many useful tools used for penetration testing. We can access those tools interface via terminal using Kali Linux Commands. Favorite penetration tools include NMAP, backtrack, MITM, etc. It matters a lot because theres no need to download and install them. Hence, its also said that Kali is heaven for ethical hackers.We should have basic knowledge ofKali Linux commands. Thats because if we know about commands, itll become easy for us to perform the tasks using the terminal. We can even install Kali Linux on USB instead of installing it on HDD. It gives us full portability and power to boot on any machine. 250+ Kali Linux Commands In 2022Here are all Kali Linux commands with examples. Ive written down their operations e.g task to be performed once the command is executed. S. No.Kali Linux CommandsFunction 1.aproposGet Help Related Documents 2.apt-getFetch Software Packages Directly From Internet 3.aptitudeIt can also be used to fetch software packages directly 4.aspellSpell Checker Command 5.awkUse to Find or Replace text 6.basenameGet the directory and suffix from filenames 7.bashGNU Bourne-Again Shell 8.bcPrecision calculator language 9.bgSend items to background 10.breakExit the command or loop running 11.builtinRun shell builtin 12.bzip2Compress files to decrease their size Extraction/Compression 13.calUsed to display current calendear 14.casePut conditions in commands like if then structure 15.catConcatenate and display data of files 16.cdBrowse through directories 17.cfdiskPartition table manipulator 18.chgrpChange ownership of group 19.chkconfigCheck system configuration 20.chmodChange the permissions 21.chownChange owner or group of files 22.chrootRun command on different directory 23.cksumPrint CRC and byte counts 24.clearClear all the things in terminal to start fresh 25.cmpCompare two files to get detailed difference 26.commUsed to compare two sorted files line by line in details 27.commandRun a command 28.continueCOntinue the loop/process 29.cpCopy files from one location to another 30.cronSchedule the commands to run at particular time 31.crontabSchedule command to run later at time 32.csplitBreak/Split files into two parts 33.cutDivide files into many parts 34.dateDisplay current date and can also change it 35.dcShow desk calculator 36.ddCopy and convert a file 37.ddrescueData recovery pool command 38.declareDeclare your variables with ease 39.dfShow up free disk space on hard drive 40.diffDifference between two files 41.diff3Difference between 3 files 42.digGet DNS Details 43.dirShow all the directory details 44.dircolorsDirectory tree color change 45.dirnameFull pathname to a path 46.dirsDisplay recent directories 47.dmesgKernel and driver messages on screen 48.duFile space usage estimation 49.echoDisplay message on screen 50.egrepFind all the files in which particular lines are contained 51.ejectUnplug external connected device 52.enableEnable and disable shell commands (builtin) 53.envEnvironment variables 54.ethtoolAdjust enternet card settings 55.evalEvaluate several commands/arguements 56.execExecute commands 57.exitExit 58.expandTabs to spaces 59.expectAutomate arbitrary applications 60.exportSet env. variables 61.exprEvaluate exp. 62.fdformatFormt a floppy 63.fdiskPartition table 64.fgSend task to foreground 65.fgrepSearch for lines that contains specific string/words 66.fileCheck file type 67.findFind files with some adjustments and criteria 68.fmtReformat paragraph 69.foldWrap text 70.forExpand words 71.formatFormat internal/external partitions 72.freeDisplay memory usage 73.fsckFile system consistency 74.ftpFile transport protocol to transfer files 75.functionDefine function 76.fuserIdentify/Kill the process accessing particular file 77.gawkFind and Replace Text 78.getoptsParse parameters which are positional 79.grepSearch files for lines in given pattern 80.groupaddAdd new user to group 81.groupdelDelete any group 82.groupmodUse it to modify group 83.groupsPrint groups you're in 84.gzipCompress files/folders 85.hashRemember full path of the name argument 86.headFirst part of file 87.helpDisplay help of any command 88.historyHistory of all commands executed so far 89.hostnamePrint system name 90.iconvConvert character set of the file 91.idPrint user or group ID 92.ifCreate if command structure 93.ifconfigShow network interface 94.ifdownStop network interface 95.ifupStart network interface 96.importCapture server screen and save 97.installInstall 98.jobsShow all active tasks 99.joinJoin lines on common field 100.killKill a process from running 101.killallKill all the processes 102.lessDisplay output of screen 103.letArithmetic shell 104.lnSymbolic link of the file 105.localCreate local variables 106.locateFind files at locations 107.lognamePrint login name 108.logoutExit login shell 109.lookDisplay lines 110.lpcLine printer control 111.lprOff line 112.lprintPrint file 113.lprintdAbort print 114.lprintqList print queue 115.lprmRemove print queue (Single Item) 116.lsList files in particular directory 117.lsofList of all the files which are currently open 118.makeRecompile programs 119.manShow help manual 120.mkdirCreate new folders 121.mkfifoMake FIFOs 122.mkisofsCREATE iso9660/joliet/hfs filesystem 123.mknodMake character files 124.mmvMove and rename files in bulk 125.moreDisplay output in one screen at a time 126.mountMount the file system 127.mtoolsManipulate MS-DOS files 128.mtrTraceroute/ping 129.mvMove files and directories 130.netstatCurrent network information 131.niceSet command priority 132.nlList number of lines 133.nohupRun command immune to hangups 134.notify-sendPush desktop notifications 135.nslookupName servers lookup 136.opOperator access 137.openOpen particular file with application assigned to it 138.passwdChange any user's password 139.pasteMerge files 140.pathchkCheck file path 141.pingPing any particular address 142.pkillStop process 143.popdRestore previous values of directory 144.prPrepare files for printing purpose 145.printcapPrint capability 146.printenvPrint environment 147.printfDisplay output 148.psProcess status 149.pushdSave & change current directory 150.pwdDisplay working directory 151.quotaDisplay quota 152.quotacheckCheck file for quota usage 153.quotactlSet disk quotas 154.ramRam disk device 155.rcpCopy file from one computer to another 156.readRead a line 157.readarrayRead the array 158.readonlySet file type to readonly to give restrictions 159.rebootReboot computer 160.remsyncSynchronize remote files 161.renameRename files 162.reniceAlter priority 163.returnExit function 164.revReverse line 165.rmRemove files 166.rmdirRemove the folders 167.rsyncSync file trees 168.scpSecure copy 169.screenMultiplex the terminal 170.sdiffCombine two files interactively 171.sedStream editor 172.selectAccept the kwyboard input 173.seqPrint sequences 174.setManipulate shell variables 175.sftpSecure FTP connection 176.shiftShift the parameters which are positional 177.shoptDisplay shell options 178.shutdownShutdown computer 179.sleepPut computer to sleep 180.slocateLocate files 181.sortSort the files 182.sourceRun commands from the file 183.splitBroke files into justified parts 184.sshLaunch remote login program 185.straceTrace calls and signals 186.suSubstitute user identity 187.sudoExecute command as another user 188.sumPrint checksum of file 189.suspendSuspend execution of file 190.symlinkMake new name for file 191.syncSync the data 192.tailDisplay last part of any file 193.tarTape Archiver (Compress Files) 194.teeRedirect output to multiple files 195.testEvaluate conditional expression 196.timeDisplay time 197.timesUser and system times 198.topList of top services running in computer 199.touchTo change file timestamps 200.trTranslate 201.tracerouteTrace back to host 202.trapRun any particular command when signal is set 203.trueNo action 204.tsortTopological sorting 205.ttyPrint terminal on stdin filename 206.typeDescribe any command 207.ulimitPut limits on user resources 208.umaskFile creation mask 209.umountUnmount the device 210.unaliasAlias removal 211.unameDisplay system information 212.unexpandSpace to tabs 213.uniqUniquify the files 214.unitsConvert units from scale 215.unsetRemove variable 216.unsharUnpack shell archive scripts 217.untilUntil condition 218.uptimeDisplay uptime of machine 219.useraddAdd new user 220.usermodModify existing user 221.usersDisplay all the users 222.uudecodeDecode a file created by uuencode 223.uuencodeBinary files encode 224.vList directory contents (`ls -l -b) 225.vdirList directory contents (`ls -l -b) 226.viDefault text editor 227.vmstatDisplay Virtual memory statistics 228.waitWait till process is complete 229.watchPeriodically display a program 230.wcDisplay byte, word, and line counts 231.wgetGet files (HTTP, HTTPS, FTP supported) 232.whereisSearch path etc. 233.whichSearch path for program 234.whileConditional statement 235.whoPrint all users which are currently logged in 236.whoamiShow current user profile 237.writeSend message to other user. 238.xargsUtility, passing constructed argument lists execution 239.xdg-openOpen file/url using default program 240.yesPrint string until any obstacle These are all the Kali Linux commands you can use inside the terminal. Ive executed all the commands using Kali, and they perform many important tasks.Keep this in mind that these commands are related to the inbuilt function of OS. If youve installed 3rd party software, make sure to check its documentation for the commands. You can only access the OSs inbuilt functions using the codes listed above in the table.Kali Linux Commands List PDF DownloadInterested people can download an offline copy of these commands. Now theres no need to visit this page again and again. Click on the Download button and save the PDF locally on your device.ConclusionAlmost all the Kali inbuilt commands are listed in this article. They can be used to perform some important task and to change inbuilt system settings as well. Ive also suggested above that these codes arent related to the third party applications but the OS itself. If youve some other interesting commands which arent listed in this article, then feel free to drop them in the comment section, and Ill add them into the article. Dont forget to share this information with your friends who take interest in penetration testing. Skip to content What is Kali Linux?Kali Linux is a Debian-based Linux distro developed by Offensive Security for penetration testing, advanced forensics and security auditing etc. It has highly customizable tools and commands that include network analyzer, password cracking tools, wireless network scanners, vulnerability scanners and so on. In a word, Kali Linux is the default OS for cybersecurity professionals.Kali Linux Commands Cheat SheetKali Linux commands cheat sheet contains many types of commands for Information Gathering, Vulnerability Analysis, and many more. Here is a list of frequently used commands of kali Linux that can be often useful for kali Linux users.Kali Linux Commands for Information GatheringKali Linux has the most extensive collection of information gathering tools and commands. These are useful for gathering information about a target system and networks. The following list has some most used tools and commands of this type. CommandDescriptionACE-voipDetect and analyze voice-over IP trafficAmapIdentify open ports and services on a remote systemAPT2Automatic penetration testing and regenerating reportsarp-scanDiscover hosts on a networkAutomaterAutomatic OSINT gatheringbing-ip2hostsEnumerate hostnames from Bing search resultbraaDetect and analyze broadcast radio signalsCaseFileCreate and manage threat intelligence reportsCDPSnarfExtract CDP information from a networkcopy-router-configBacking up router configurations or transferring configurations to a new routerDMitryGather target network information including port scanning and WHOIS lookupsdnmapIdentify hosts and services on a networkdnsenumGather information about DNS records including subdomainsdnsmapIdentify active DNS servers and associated hostnamesDNSReconDNS reconnaissance tool to gather information about servers, zone transfer and IP addressesdnstracerTrace DNS queries to identify problems and misconfigurationsdnswalkCheck common DNS misconfigurationDotDotPwnExploit directory traversal vulnerabilitiesenum4linuxGather information from Windows and Samba systems including shares, users and passwordsenumIAXGather information from IAX-based VoIP systemsEyeWitnessGenerate screenshots of web applicationsFaradayManage and collaborate on vulnerability scans and security assessmentFierceIdentify non-contiguous IP space and map network infrastructureFirewalkDetermine specific traffic blocking by firewall and by analyzing TTl valuesfragroute/fragrouterIntercept and modify network traffic at IP fragmentation levelGhost PhisherSecurity testing for phishing attacksGoLismeroWeb security testing toolgoofileSearch specific file types on a target domainident-user-enumIdentify user accounts on systems that use the Ident protocolInSpyLinkedIn reconnaissance tool to gather information about employees, companies and job postingsInTraceTrace the route of TCP packets through a networkiSMTPTest the security of SMYP serverslbdIdentify load balancers and web application firewallsMaltego TeethIdentify connections and relationships between entitiesmasscanA fast port scanner used for vulnerability assessmentMetagoofilGather information and extract metadata from public documentsMirandaTool for exploiting UPnP devicesnbtscan-unixwizScan NetBIOS nameservers to gather information about connected devicesNiktoWeb server scannerntopNetwork traffic monitoring and analysisOSRFrameworkIntelligence gathering framework used for data miningp0fPassive network traffic analysis for identifying the operating systems and applications used on networked devicesParseroIdentify input validation-related vulnerabilities of web applicationsSETTool for performing social engineering attacks, password attacks etc.SMBMapEnumerate and scan SMB sharessmtp-user-enumEnumerate usernames on a target SMTP serversnmp-checkEnumerate and check the security of SNMP devicesSPARTAGraphical interface for network infrastructure penetration testingsslcauditAudit SSl/Tls certificates on a web serverSSLsplitIntercept and decrypt SSL/TLS trafficsslstripTool for performing man-in-the-middle attacks on SSL/TLS encrypted connectionsSSLyzeTest SSL/TLS servers and clientsSublist3rEnumerate subdomains of a target domain using search enginesTHC-IPV6Attack and test IPv6 networkstheHarvesterGather information on a target domain from various public sourcesTLSSLedEvaluate the security of SSL/TLS connectionstwofiFind potential usernames and passwords from TwitterUnicornscanA fast and powerful network scanning toolURLCrazyGenerate and test domain typos and variationsWiresharkNetwork protocol analyzer for capturing and analyzing network trafficWOL-ETool for Wake-On-LAN attacks and network discoveryXplicoExtract application data from network traffic Kali Linux Commands for Vulnerability AnalysisVulnerability analysis tools and commands in Kali Linux help identify the vulnerability in systems and networks, test the strength of passwords, and simulate attacks to determine potential weaknesses. Here is a list of popular tools and commands that are frequently used for vulnerability analysis. CommandDescriptionBBQSQLA blind SQL injection and exploitation toolBEDA network protocol fuzzing toolcisco-global-exploiterExploit vulnerabilities in Cisco devicescisco-ocsScan and exploit Cisco devicescisco-torchTest and scan the security of Cisco devicescopy-router-configBack up and restore Cisco router configurationsDoonaTest the security of network devices and protocolsDotDotPwnExploit directory traversal vulnerabilitiesHexorBaseA database management and exploitation tooljSQL InjectionA SQL injection exploitation toolLynisA security auditing and hardening tool for Linux and Unix-based systemsNmapNetwork exploration and security auditing toolohrwurmA local root exploitation toolopenvasA vulnerability scanner and management toolOscannerScan Oracle databases for vulnerabilitiesPowerfuzzerA web application fuzzing and discovery toolsfuzzA protocol fuzzer and vulnerability scannerSidGuesserIdentify valid user accounts in Windows domainsSIPArmyKnifeTest the security of VoIP systemssqlmapA SQL injection exploitation toolSqlninjaA SQL server injection and takeover toolsqlsusIdentify and exploit SQL injection vulnerabilitiestnscmd10gTest and exploit Oracle TNS Listener vulnerabilitiesunix-privesc-checkIdentify privilege escalation vulnerabilities in Unix-based systemsYersiniaNetwork protocol analyzer and attack tool for testing network security Kali Linux Commands for Wireless AttacksDifferent techniques such as sniffing, spoofing, and cracking of wireless encryption protocols can be used for wireless attacks. There are a lot of commands and tools in Kali Linux for applying these techniques. The following list contains the most useful ones. CommandDescriptionAirbase-ngConfigure and attack wireless access pointsAircrack-ngAudit and test wireless networkAirdecap-ng and Airdecloak-ngDecrypt and deobfuscate captured wireless trafficAireplay-ngInject traffic to wireless networks to test their securityairgraph-ngGenerate graphs from wireless network dataAirmon-ngEnable and Disable monitor mode on wireless interfacesAirodump-ngCapture wireless traffic and analyze itairodump-ng-oui-updateUpdate the OUI databases used by airodump-ngAirolib-ngManage and crack password hashes for WPA and WPA2Airserv-ngRun a wireless access point on a Linux systemAirtun-ngCreate encrypted tunnels over wireless networksAsleapCrack MS-CHAPv1 and MS-CHAPv2 authentication protocolsBesside-ngCapture and crack WEP and WPA-encrypted wireless trafficBluelogScan and log Bluetooth devicesBlueMahoDiscover and attack Bluetooth devicesBluepotSimulate Bluetooth honeypots to detect and track attackersBlueRangerControl Bluetooth devices remotelyBluesnarferExploit Bluetooth vulnerabilities and gain unauthorized access to devicesBullyBrute-forcing WPS pins to gain access to wireless networkscoWPAttyCrack pre-shared keys for WPA-PSK networkscrackleCrack encrypted Bluetooth trafficeapmd5passCrack MD5 hashes of EAP passwordsEasside-ngCrack WEP and WPA-encrypted wireless trafficFern Wifi CrackerAudit and crack wireless networksFreeRADIUS-WPEExploit weak credentials in the FreeRADIUS serverGhost PhisherCreate phishing attacks on wireless networksGISKismetMap and analyze wireless networks using GPS dataGqrxA receiver for exploring wireless signalsgr-scanscan and decode various radio signalshostapd-wpeTest and exploit the WPE feature in HostpadivstoolsConvert and manipulate IVs for WEP crackingkalibrate-rtlCalibrate the frequency offset of RTL-SDR donglesKillerBeeExplore and exploit ZigBee and IEEE 802.15.4 networksKismetDetect and analyze wireless networksmakeivs-ngGenerate and inject fake IVs for WEP crackingmdk3Attack wireless networks by flooding them with de-authentication, disassociation, and other packetsmfcukCrack Mifare Classic RFID cardsmfocCrack Mifare Classic RFID cardsmftermInteract with RFID cardsMultimon-NGDecode various radio signalsPacketforge-ngCreate and inject custom packets into wireless networksPixieWPSExploit the WPS design flaw to recover WPA/WPA2 passwordsPyritPerform advanced WPA/WPA2 password cracking using GPU powerReaverA tool for brute-forcing WPSredfangA Bluetooth scanner and vulnerability assessment toolRTLSDR ScannerA radio scanner for spectrum analysis and monitoringSpooftoophA tool for Bluetooth device spoofing and cloningTkiptun-ngWPA encryption key recovery using TKIP vulnerabilitiesWesside-ngAutomated wireless network hacking for WEP, WPA and WPA2 encryptionWifi HoneyPerform honey spot attacks on wireless networkswifiphisherSteal credentials of wireless networkWifitapCreate virtual wireless access points and monitor network trafficWifiteAudit and attack the automated wireless networkwpacleanFilter and clean WPA/WPA2 handshake capture file Kali Linux Forensics ToolsThere are a lot of specially designed tools and commands for digital forensics investigations pre-installed in Kali Linux. These allow forensic analysts to acquire, analyze, and preserve digital forensic evidence quite efficiently. Here is a brief list of these types of tools and commands. CommandDescriptionBinwalkAnalyze and extract firmware imagesbulk-extractorExtract artifacts from binary filesCapstoneA multi-platform, multi-architecture disassembly frameworkchntpwReset passwords on Windows systemsCuckooAn automated malware analysis systemdc3ddA tool for imaging and wiping hard drivesddrescueRescuing data from damaged disksDFFA forensic framework for analyzing digital evidencediStorm3A disassembler library for x86/AMD64DumpzillaAnalyze Mozilla browser historyextundeleteRecover deleted files from ext3/ext4 partitionsForemostExtract files from disk imagesGalletaAnalyze browser cookiesGuymagerCreate forensic imagesiPhone Backup AnalyzerAnalyze iPhone backups.p0fA tool for passive OS fingerprinting and network analysispdf-parserA tool for analyzing PDF filespdfidAnalyze and detect malicious PDF filespdgmailAnalyze Gmail artifactspeepdfAnalyze and explore PDF filesRegRipperAnalyze Windows registry hivesVolatilityAnalyze memory dumps Kali Linux Exploitation ToolsYou can employ the exploitation tools of Kali Linux to develop and execute a wide range of exploits, from simple command injection attacks to complex remote code execution exploits. The following list contains most used exploitation tools of Kali Linux. CommandDescriptionArmitageA graphical cyber attack management toolBackdoor FactoryAdd backdoors to binariesBeEFPenetration testing focuses on browser-based attacksCommixA command injection exploitation toolcrackleBreak Bluetooth Smart encryptionexploitdbA database of known exploits and vulnerable softwarejboss-autopwnExploit vulnerabilities in JBoss serversMSFPCCreate Metasploit payloadsRouterSploitTest vulnerabilities in routers and other embedded devicesShellNoobGenerate shellcode and convert shellcode to assembly Kali Linux Hardware Hacking ToolsThe hardware hacking tools and commands are useful to identify and exploit vulnerabilities in various hardware devices. The list below contains a few of those. CommandDescriptionandroid-sdkA software development kit for developing Android applicationsArduinoAn open-source electronics platform for creating interactive projectsdex2jarConvert Android DEX files to Java JAR filesSakis3GConnect to 3G mobile networkssmaliAn assembler/disassembler for Androids dex format Reverse Engineering in Kali LinuxIn Kali Linux, there are several powerful tools and commands available for reverse engineering tasks. You can use these to disassemble, decompile, and analyze binaries. Here is a short list of a few of those. CommandDescriptionapktoolReverse engineer and modify Android APK filesdiStorm3A disassembler library used for binary analysisedb-debuggerA cross-platform debugger for x86, ARM, MIPS, and PowerPC executablesjadAnalyze and reverse engineer Java bytecodejavasnoopIntercept and analyze Java method callsJD-GUIDecompile and analyze Java bytecodeOllyDbgA 32-bit assembler-level analyzing debuggerValgrindDebug and profile Linux programsYARAMatch patterns and identify malware and other suspicious files Web Applications in Kali LinuxThere are various tasks including identifying web vulnerabilities, misconfiguration, and security issues in web applications. Kali Linux is well-equipped to handle all of these. You can frequently use the following commands and tools to handle different issues related to web applications. CommandDescriptionapache-usersFind usernames on an Apache web serverArachniA feature-rich web application security scannerBlindElephantIdentify the web applications version numberBurp SuiteWeb application testing frameworkCutyCaptCapture website screenshotsDAVTestTest the security of WebDAV serversdeblazeDiscover hidden files and directories on a web serverDIRBA tool used for web content discoveryDirBusterA multi-threaded web application scannerfimapAutomate web application attacks and vulnerability scanningFunkLoadA web functional testing and load testing toolGobusterBrute forcing directories and files on web serversGrabberDetect security vulnerabilities of web applicationshURLA tool used for web application testing and discoveryjboss-autopwnExploit vulnerable JBoss application serversjoomscanIdentify vulnerabilities in Joomla! CMSPadBusterTest Padding Oracle vulnerabilities in web applicationsParosA web application testing proxy used to intercept and analyze web trafficParseroA tool used for web application fingerprinting and directory discoveryplecostA WordPress vulnerability scannerPowerfuzzerA highly automated web application vulnerability scannerProxyStrikeAttack web applications through proxiesRecon-ngA web reconnaissance frameworkSkipfishA web application security scanner used for reconnaissance and discoveryua-testerTest user-agent strings in web applicationsUniscanSecurity scanner used for finding vulnerabilitiesw3afA framework used for web application security testingWebScarabA Java-based web application testing proxy used for intercepting and analyzing web trafficWebshagA multi-threaded, multi-platform web application vulnerability scannerWebSlayerFind vulnerabilities in web applicationsWebSploitA web application security testing frameworkWfuzzA web application fuzzer used for brute forcing directories and files on web serversWhatWebFingerprint web servers and identify vulnerabilitiesWPScanA WordPress vulnerability scannerXSSerFind and exploit XSS vulnerabilities Stress Testing in Kali LinuxStress testing is crucial and depicts the resilience of a system against any cyber-attacks. A few commands and tools of Kali Linux related to stress testing are listed below. CommandDescriptionDHCPigFlood DHCP servers with requests, causing them to crash or become unavailableiaxfloodFlood SIP servers with requests, causing them to crash or become unavailableInundatorFlood a network with random packets, causing network congestion and slowdownsinvitefloodFlood SIP servers with INVITE requests, causing them to crash or become unavailableipv6-toolkitCollection of tools for testing and exploiting IPv6 networksrtpfloodFlood VoIP servers with RTP packets, causing them to crash or become unavailableSlowHTTPTestTest the vulnerability of web servers to Slow HTTPt50Generate network traffic and test the performance of network devices under heavy loadsTermineterTest the security of Smart Grid devices and protocolsTHC-SSL-DOSFlood SSL servers with SSL handshake requests, causing them to crash or become unavailable Sniffing & Spoofing in Kali LinuxSniffing and spoofing are two common techniques to intercept and manipulate network traffic. Kali Linux offers a variety of commands and tools for sniffing and spoofing detection. Look over some of the commonly used sniffing and spoofing commands and tools listed below. CommandDescriptionSIPpTest and benchmark SIP-based VoIP systemsrtpbreakDetect, reconstruct, and analyze RTP sessionsSIPViciousAudit SIP-based VoIP systemsrtpmixsoundMix audio into RTP streamsbettercapA Swiss Army knife for network attacks and monitoring, including sniffing, spoofing, and MITM attacksDNSChefA DNS proxy that can be used to forge DNS responses and redirect traffic to malicious sitesfikedA fake IKE daemon used for launching MITM attacks against IKEv1-encrypted connectionshamster-sidejackPerform session hijacking attacks against web applicationsHexInjectCraft and inject packets into a networkiSMTPTest the security of SMTP servers by sending a large number of emailsisr-evilgradeExploit software vulnerabilities and perform automatic updates of malicious softwaremitmproxyA SSL-capable intercepting proxy used for intercepting, modifying, and replaying traffic between clients and serversohrwurmGenerate payloads and test the detection capabilities of antivirus softwareprotos-sipTest the security of SIP-based VoIP systemsrebindPerform DNS rebinding attacks against web applicationsresponderSteal NTLMv1/v2 hashes and perform LLMNR/NBT-NS poisoningrtpinsertsoundInsert audio into RTP streamssctpscanPerform SCTP network scanning and fingerprintingSIPArmyKnifeA tool used for testing the security of SIP-based VoIP systemsSniffJokeManipulate network traffic in real-timeVoIPHopperDetect and exploit VoIP security vulnerabilitiesxspyMonitor and analyze X11 trafficzaproxyTest the security of web applications by scanning Kali Linux Reporting ToolsIt is essential to generate an accurate report of penetration testing and provide it to clients and stakeholders for mutual understanding about the security risk of a system. Kali Linux has tools like Dradis, MagicTree etc. for managing, visualizing and reporting results of penetration testing. CommandDescriptionCaseFileCreate diagrams and charts to aid in the organization and visualization of data during investigationscherrytreeA hierarchical note-taking application that allows the creation and organization of notes and code snippetsCutyCaptCapture screenshots of web pages from the command linedos2unixConvert DOS-style line endings to Unix-style line endings in text filesDradisA collaboration and reporting platform for security testing professionalsMagicTreeVisualize and analyze data from different sources, such as file systems, network traffic, and databasesNipper-ngA tool used for auditing network device security configurationspipalA password analyzer and cracking tool used to identify weak passwordsRDPYPerform remote desktop protocol operations, such as screen capture and input injection Password Attacks in Kali LinuxDifferent types of password attacks are common for hackers to gain unauthorized access to systems or networks. Using tools and commands of Kali Linux, professionals can test security and vulnerabilities related to passwords. CommandDescriptionBruteSprayAutomate password spraying attacks against multiple hosts simultaneouslyCeWLGenerate custom wordlists for password cracking and other security assessmentschntpwReset passwords on Windows systems by modifying the Windows registryCmosPwdRecover CMOS passwords on Windows systemscreddumpExtract password hashes and other credentials from Windows systemscrowbarBrute-force attacks against remote authentication servicescrunchGenerate custom wordlists for password cracking and other security assessmentsfindmyhashIdentify the hash algorithm used to encrypt password hashesgpp-decryptDecrypt Group Policy Preferences (GPP) passwords on Windows systemshash-identifierIdentify the type of hash used to encrypt password hashesHashcatA tool used for advanced password cracking and recoveryHexorBaseA tool used for database management and exploitationTHC-HydraBrute-force attacks against remote authentication servicesJohn the RipperA tool used for password cracking and recoveryJohnnyA graphical user interface for John the Ripper password-cracking toolkeimpxExploit vulnerabilities in Microsoft Windows systemsMaskprocessorGenerate custom wordlists based on specified criteriaNcrackBrute-force attacks against remote authentication servicesoclgausscrackAdvanced password cracking and recovery on systems with OpenCL-compatible hardwareophcrackPassword cracking and recovery on Windows systemsPACKAdvanced password cracking and recoverypatatorBrute-force attacks against multiple protocols and servicesphrasendrescherGenerate custom wordlists based on natural language patternspolenumRetrieve password policy information from Windows systemsRainbowCrackAdvanced password cracking and recovery using rainbow tablesSecListsA collection of various security-related wordlists for password cracking and other security assessmentsSQLdictGenerate custom wordlists based on SQL queriesStatsprocessorGenerate custom wordlists based on a statistical analysis of existing passwordsTHC-pptp-bruterBrute-force attacks against PPTP VPNsTrueCrackA tool used for advanced password cracking and recoverywordlistsCollection of various wordlists for password cracking Maintaining Access in Kali LinuxA list of useful Kali Linux tools and commands for bypassing security measures and maintaining access to a system is below. CommandDescriptionCryptCatCreate encrypted and authenticated connections between two hostsCymothoaInject shellcode into a running process in order to gain remote accessdbdA backdoor daemon that allows remote access to a system via a network connectiondns2tcpA tool used to tunnel TCP traffic over DNS protocolsHTTPTunnelA tool used to tunnel traffic over HTTP protocolsIntersectGenerate payloads for exploitation of vulnerabilitiesNishangCreate and execute PowerShell scripts for penetration testingPowerSploitCollection of PowerShell scripts for penetration testing and other security assessmentspwnatBypass NAT firewalls and establish direct connections between two hostsRidEnumEnumerate user accounts and groups on Windows systemssbdCreate a secure backdoor connection between two hostsshellterBypass antivirus software and other security mechanismsU3-PwnExploit security vulnerabilities in U3 USB smart drivesWebshellsCollection of scripts and tools used for remote access and exploitation of web serversWeevelyA web shell is used to gain remote access to web servers and execute commandsWinexeRemotely execute commands on Windows systems from a Linux or Unix host ConclusionThe Kali Linux commands are useful for testing the security of systems and networks and identifying vulnerabilities by attackers. I believe the compact list may become useful for professionals to recall perfect commands and employ proper tools whenever necessary. Please feel free to comment below if you find the list helpful or have any suggestions regarding it. Visit linuxsimply for the most useful articles and cheat sheets. Kali Linux has gained widespread popularity, especially among younger tech enthusiasts, thanks in part to its prominent feature in pop culture including shows like Mr. Robot. But beyond the allure of Hollywood, Kali Linux is a powerful, security-focused operating system with tools tailored for penetration testing and cybersecurity. Whether you're a beginner curious about ethical hacking or a budding cybersecurity professional, Kali Linux offers a unique environment to learn and practice advanced security techniques. Kali Linux is ideal for those focused on cybersecurity because it provides a complete suite of tools that would otherwise require complex installation on standard operating systems. Its primary users include penetration testers, cybersecurity analysts, and IT professionals who regularly deal with security challenges. Ready to learn Kali Linux? Enroll in our online cybersecurity bootcamp to get started. What is Kali Linux? Kali Linux is a powerful, security-focused Linux distribution tailored for digital forensics, ethical hacking, and penetration testing. Developed by cybersecurity experts Devon Kearns and Mati Aharoni at Offensive Security, Kali Linux was introduced as a successor to the popular BackTrack distribution, incorporating significant improvements to better meet the demands of modern cybersecurity professionals. Unlike general-purpose Linux distributions, Kali Linux is purpose-built for cybersecurity. It is preloaded with over 600 advanced tools, designed for tasks like vulnerability assessment, network scanning, password cracking, reverse engineering, and forensic analysis. Each of these tools has been carefully curated to support security practitioners in identifying and mitigating risks across various digital environments. One of the standout features of Kali Linux is its highly customizable and flexible architecture. Its designed to operate across various hardware setups, from traditional desktop computers to ARM-based devices like Raspberry Pi, which makes it accessible and practical for professionals in diverse settings. Kali Linux also offers several deployment options, including installation on hard drives, USB live boot, or virtual machines, making it a portable and adaptable solution for penetration testers and security analysts on the move. Kali Linux comes with over 600 pre-installed security and penetration testing tools, including: Exploitation Tools Forensics Tools Hardware Hacking Information Gathering Maintaining Access Password Attacks Reporting Tools Reverse Engineering Sniffing & Spoofing Stress Testing Vulnerability Analysis Web Applications Wireless Attacks Recent Kali Linux 2024.3 Update The Kali Linux 2024.3 update brings a suite of powerful new tools and significant enhancements, reinforcing its reputation as a top choice for penetration testers and cybersecurity professionals. With the addition of 11 new tools, improved support for ARM devices, and essential behind-the-scenes optimizations, this update positions Kali Linux as an even more robust platform for security work. Heres a closer look at whats new in the 2024.3 release. The 2024.3 update introduces a collection of innovative tools designed to address various security tasks, making Kalis toolkit even more comprehensive. Key additions include: Hekatomb: A versatile credential extraction tool, Hekatomb is designed to locate and decrypt sensitive credentials from compromised systems, supporting penetration testers and forensic investigators in gathering key insights on network access and security vulnerabilities. NetExec: This network service exploitation tool streamlines the process of identifying and exploiting vulnerable network services, helping testers simulate real-world attacks to understand the potential impact of network weaknesses. SprayHound: An advanced password spraying tool with seamless integration into Bloodhound, SprayHound simplifies testing password policies by allowing users to spray passwords across Active Directory domains. Its especially useful for simulating password-based attacks in a controlled environment, giving insight into an organizations password security. Enhanced Support for ARM Devices and Raspberry Pi Kali Linux has long supported ARM devices, but the 2024.3 update takes this compatibility further, optimizing the system to run more efficiently on low-power devices like Raspberry Pi. This enhancement is particularly useful for security professionals who require a portable, lightweight solution for fieldwork, as it allows them to leverage Kali Linux on ARM-based hardware without sacrificing performance. With improved device compatibility and power efficiency, the update makes Kali Linux a versatile choice for those who need flexibility in their security setups. Behind-the-Scenes Improvements and Optimizations In addition to the new tools and enhanced ARM support, the 2024.3 update includes a host of behind-the-scenes improvements aimed at optimizing Kali Linuxs performance and stability. These adjustments make the OS faster and more reliable, ensuring that it can handle the demands of intensive security operations. The update refines everything from tool performance to system stability, reinforcing Kali Linux as the go-to choice for security professionals who need a dependable, high-performance platform for penetration testing. With this update, Offensive Security has further solidified Kali Linuxs position as the industry-standard OS for penetration testing, demonstrating a commitment to meeting the needs of cybersecurity professionals worldwide. As threats evolve, Kali Linux continues to keep pace, equipping users with the latest tools, improved compatibility, and a smooth, stable environment for conducting advanced security assessments. Why Do Hackers Use Kali Linux? Kali Linux has become the preferred operating system for ethical hackers, security professionals, and cybersecurity enthusiasts due to its specialized focus on penetration testing, digital forensics, and security analysis. Unlike general-purpose operating systems, Kali Linux is purpose-built with a suite of powerful, carefully curated tools that streamline the ethical hacking process, enabling users to focus directly on core security testing and investigative tasks without the clutter of unnecessary software. One of the major advantages of Kali Linux is its pre-installed selection of security tools. With over 600 tools readily available, including Nmap, Metasploit, Wireshark, and Aircrack-ng, users have immediate access to a wide range of functionalities for tasks such as network scanning, vulnerability assessment, password cracking, and wireless network analysis. This collection minimizes setup time and eliminates the need for downloading or configuring separate tools, allowing security professionals to jump straight into testing and analysis. Kali Linux also offers an efficient, customizable environment that makes it adaptable to different hacking tasks. Users can run Kali on various platforms, from desktop systems to lightweight ARM devices like Raspberry Pi, making it a versatile option for both fieldwork and controlled environments. Its flexibility is particularly useful for hackers and security analysts who need an OS that can handle different testing setups without extensive reconfiguration. Common Uses of Kali Linux Kali Linux has established itself as a powerful, versatile platform for a wide range of cybersecurity and IT-related tasks. Designed specifically for security professionals, it provides tools and capabilities that make it essential for activities like security auditing, forensics, and penetration testing. Heres a closer look at the most common uses of Kali Linux and why its trusted by cybersecurity experts worldwide: 1. Security Auditing One of the primary uses of Kali Linux is for security auditing. Security professionals and IT administrators use it to assess the strength of networks, systems, and applications by simulating attacks, identifying vulnerabilities, and ensuring compliance with security policies. With built-in tools like Nmap for network scanning, Nikto for web server analysis, and OpenVAS for vulnerability scanning, Kali Linux allows auditors to evaluate and report on the overall security posture of an organization. Through regular audits, teams can proactively address weaknesses and reinforce defenses, maintaining a secure infrastructure. 2. Digital Forensics and Incident Response (DFIR) Kali Linux also plays a significant role in digital forensics and incident response (DFIR), making it a valuable resource for forensic investigators and analysts. When breaches occur, Kali Linux can be used to perform reverse engineering, trace data trails, and recover lost information. Forensic tools like Autopsy, Binwalk, and Foremost aid in analyzing disk images, extracting hidden files, and recovering data from damaged or corrupted systems. These capabilities help forensic teams understand the extent of an attack, piece together the sequence of events, and collect evidence for further investigation or legal proceedings. 3. Penetration Testing Penetration testing, or pen testing, is one of the most common applications of Kali Linux. Ethical hackers use Kali to mimic real-world attacks, testing the resilience of networks, applications, and devices by attempting to exploit vulnerabilities. With tools like Metasploit for exploit development, Hydra for brute-force attacks, and Burp Suite for web application testing, Kali Linux provides everything required to conduct thorough penetration tests. By identifying weak points and exploiting them in a controlled setting, ethical hackers can help organizations strengthen their defenses and better prepare for potential threats. Legal and Ethical Considerations Kali Linux is a completely legal operating system, specifically designed for cybersecurity tasks such as penetration testing, digital forensics, and security research. Developed by Offensive Security, it is intended to be used by ethical hackers and security professionals to identify and secure vulnerabilities within networks, applications, and devices. However, while Kali Linux itself is lawful and serves a critical role in bolstering cybersecurity defenses, its use becomes illegal when applied for unauthorized or malicious purposes, such as hacking into systems without consent. In essence, the legality of using Kali Linux lies in how, where, and why its used. Target Audience for Kali Linux Kali Linux is designed with a specific audience in mind: professionals in the cybersecurity field, including ethical hackers, penetration testers, security researchers, and forensic analysts. Its suite of pre-installed, advanced tools caters to those focused on identifying vulnerabilities, testing defenses, and conducting digital investigations. Due to the technical nature of these tools and the OSs command-line-driven interface, Kali Linux may present a steep learning curve for beginners or those unfamiliar with Linux systems. As a result, Kali Linux is not generally recommended for casual users or newcomers to cybersecurity. However, those with specific training goals, a strong interest in learning cybersecurity, or a clear educational focus may find Kali Linux to be a powerful platform for hands-on experience in the field. Windows Compatibility With the Windows Subsystem for Linux (WSL), users can run Kali Linux tools directly on a Windows 10 or 11 system, creating a convenient environment for those who rely on Windows but want access to Kalis cybersecurity toolkit. WSL integration allows users to execute many of Kalis command-line tools, enabling basic penetration testing, security audits, and vulnerability assessments without needing to dual-boot or install a virtual machine. However, its important to note that some advanced features, like full wireless and USB support, may be limited or unavailable when running Kali on WSL. This setup is ideal for users who need light, on-the-go access to Kali tools on a Windows system, but for comprehensive penetration testing and full feature functionality, a native or virtual installation of Kali Linux is recommended. Methods to Install Kali Linux There are several ways to install Kali Linux on your machine. These methodologies include: Cloud Installation: Kali Linux is available on cloud platforms like Microsoft Azure and Amazon AWS. Direct Installation with ISO Image: Installing Kali Linux directly on a computer or laptop, particularly on Wi-Fi-enabled systems, for full functionality. Mac: Dual or single booting on Mac systems is also supported. USB Boot Disk: Use a bootable USB to run Kali Linux without installation. Virtualization: Install Kali Linux using virtual machines (VMs) such as Oracle VirtualBox, VMware, or Hyper-V. Windows 10 (App): Kali Linux can be installed natively on Windows 10, though some features may still be in beta. How to Install Kali Linux with VirtualBox (Step-by-Step Guide) This guide provides a detailed, step-by-step walkthrough on how to install and run Kali Linux on Oracle VirtualBox. From downloading the Kali Linux OVA file to importing and launching the appliance, youll be set up to explore Kalis powerful features within a virtual environment. 1. First, visit this site to access the download file. 2. Next, select an OVA image and download it. Import that OVA image to VirtualBox. 3. Open the Oracle VirtualBox Application. Go to File, Menu and then select the option to Import Appliance. 4. A window will open on your screen, titled Appliance to Import. Go to, and click on, the destination where youve saved the OVA image. 5. After clicking the Open button, you will return to the Appliance to Import window. Click Next. 6. An Appliance Settings window will open on your screen. This window will show an outline of the systems settings. Note the location of Virtual Machine on your machine. Select Import once done. 7. VirtualBox will now import the Kali Linux OVA appliance onto your system. It will take 7-10 minutes to finish. 8. Congratulations! You have successfully installed Kali Linux on VirtualBox. You should now be able to view the Kali Linux VM in the VirtualBox Console. 9. To boot up the Kali Linux Operating System, click on the Kali Linux VM inside the VirtualBox Dashboard, and then click on the Start button. 10. A login screen will appear. Type Root as the username, and move to the next step by clicking Next. 11. Type toor as the username and click Sign In. Advantages and Disadvantages of Kali Linux Kali Linux offers powerful tools and capabilities for cybersecurity professionals, making it a top choice for penetration testing, forensics, and network security. However, its specialized focus and technical requirements mean it may not be suitable for everyday users or those unfamiliar with Linux. Advantages Kali Linux has several distinct advantages. These include: Over 600 pre-installed penetration testing tools. Free and open-source distribution. Extensive language support. Compatibility with RaspberryPi. Disadvantages Kali Linux also has a few disadvantages. These include: Not recommended for Linux beginners. Slower compared to other distributions. May have compatibility issues with some software. Should You Use Kali Linux? Kali Linux is a powerful, security-focused operating system, but its suitability varies depending on your experience level and goals. Beginners may benefit from first exploring general Linux distributions like Ubuntu or Debian, which offer a more user-friendly interface and can help build foundational Linux skills before transitioning to Kalis more complex, security-oriented environment. Advanced users such as security professionals and ethical hackers will find Kali Linux ideal for penetration testing, vulnerability analysis, and digital forensics, though it requires a solid understanding of Linux and cybersecurity principles to use effectively. Windows users can take advantage of Kali tools via the Windows Subsystem for Linux (WSL), which allows them to integrate Kalis capabilities directly on their Windows systems. This can be a convenient option for those who want to start experimenting with Kalis toolkit without dedicating a separate device or installing it on a virtual machine. Ultimately, Kali Linuxs extensive collection of security tools makes it an invaluable asset for anyone serious about cybersecurity, from penetration testers to forensic analysts, but its best suited for users with a focused purpose and familiarity with security workflows. Want to dive into cybersecurity? Explore our Cybersecurity Bootcamp to boost your cybersecurity skills and prepare for a successful career. Previously known as Backtrack, Kali Linux promotes itself as an increasingly cleaned replacement with all the more testing-driven tools, dissimilar to Backtrack which had numerous tools that would fill a similar need, thusly, making it stuffed with pointless utilities. This smooths out the process of ethical hacking using Kali Linux. Kali Linux is a powerful and versatile operating system specifically designed for penetration testing, security auditing, and digital forensics. It comes preloaded with a wide array of specialized tools that make it an essential platform for cybersecurity professionals, ethical hackers, and security researchers.While Kali Linux functions as a standard operating system, its the extensive suite of tools that truly sets it apart, offering everything you need for testing the security of networks, systems, and applications. When you first install Kali Linux, you can use it just like any other Linux distribution. However, to truly unlock its potential, youll need to dive into the diverse set of utilities it includes.Kali comes equipped with hundreds of tools, many of which serve similar purposes. While it may seem overwhelming at first, you dont need to master every single tool. In fact, many of the tools are alternatives to one another, designed to accomplish the same tasks in different ways.The key to effectively using Kali is understanding the range of tools available, how they function, and selecting the right ones for your specific needs. Once you grasp which tools are most effective for each task, youll be able to focus on mastering those and applying them in real-world security assessments. In this guide, well introduce you to Kali Linux and help you navigate its powerful features.About Kali LinuxThe most amazing feature of Kali Linux is its price it is free to use. Despite being packed with tools, you dont have to pay anything to download and use it. The secret behind this giveaway is that all of the components of the Kali package are individually free. The creators of Kali sought out useful free systems and packaged them together.The main element in Kali is the Linux operating system. This is taken from Debian Linux. If you arent interested in penetration testing, then you probably should install Debian Linux instead of Kali because you will be using the same operating system.Although Kali is given away for free, it is actually owned by a business. The system is a product of Offensive Security. This organization has created a number of open-source projects. All of those systems are free to use. The company makes its money by providing consultancy services. Essentially, Offensive Security is a cybersecurity business that created bundles of tools for its consultants and customers to use and made those bundles available to the world.Many of the tools in the Kali bundle are also open-source projects. These are run by volunteers and many IT professionals and cybersecurity professionals contribute to the development of these systems for free. They get the prestige associated with these tools and that advances their careers, so there is a business logic behind getting involved in these projects and they attract very skilled and respected contributors.Acquiring Kali LinuxGo to the website for the Kali project in order to find out more about Kali Linux. You can just go straight to the Kali Linux download page if you just want to get on with installing the system.The service offers eight different installation options, including versions that can be run on Android devices, on VMs, and on containers. The most popular option is to install the software on a bare-metal computer.Whichever installation option you choose, you will find an installation guide in the section that includes the download file.Kali Linux has a graphical user interface you dont have to work at the command line all of the time.Not all of the tools included in the system work through the interface, though. Some of them are only available at the command line.There are about 300 tools built into Kali Linux in addition to the Debian operating system. All of the tools are focused on pen-testing. In this guide, we will look at just the 20 most significant tools that you can find within the Kali Linux package.You can see a full list of the penetration testing tools in Kali Linux in our PDF.This is a JPG image, download the PDF below to retain the clickable hyperlinks.Click on the image above to open the Kali Linux Cheat Sheet PDF in a new window. Each tools name is a link through a website that explains the functions of the utility.The tools that we will look at in this guide are:Aircrack-ng A packet sniffer for wireless LANs.Autopsy A graphical interface to The Sleuth Kit, which aids forensic exploration of hard disks.Armitage A front end for Metasploit tools that manages attack strategies.Burp Suite A system that launches man-in-the-middle attacks and includes password cracking.BeEF The Browser Exploitation Framework tries to break into servers through websites.Cisco Global Exploiter Attacks Cisco routers and switches.Ettercap A traffic interceptor designed for man-in-the-middle attacks.Foremost A command-line disk copying and file recovery tool.Hashcat A password cracker.Hydra A password cracker.John the Ripper A command-line password cracker.Kismet A network scanner, packet sniffer, and intrusion detection system for wireless networks.Maltego A data discovery tool that maps relationships between data, including network layouts, social media connections, and software dependencies.Metasploit Framework Scans targets for endpoints and then builds attacks based on discovered knowledge.Nikto A command-line Web vulnerability scanner.Nmap A command-line network scanner and device discovery tool.OWASP ZAP The Zed Attack Proxy is a Web vulnerability scanner and traffic interceptor.sqlmap A command-line service for web vulnerability scanning and password cracking.Wireshark A world-famous packet sniffer.WPScan A vulnerability scanner for WordPress sites.These are the most useful tools in the Kali bundle that you will probably use all the time when pen-testing. If you dont want to bother installing the full Kali package that includes all of the other tools, you could just install Debian Linux and each of these tools individually because they are all available for free. The links in the tool names in the above list will take you through to the home page for that system.You can read more about each of these tools in the following sections.1. Aircrack-ngAircrack-ng offers detection of wireless signals and it can extract data as it passes along a selected channel. The system allows you to export captured packets for analysis in another tool. The Aircrack-ng utility is a command-line system and it displays its output in multi-colored characters to aid data comprehension.The Aircrack-ng features include the ability to crack passwords, but only on systems with weak security (WEP, WPA 1, WPA 2). It is also able to broadcast packets into a stream, which allows it to perform a variety of attacks. These include replay attacks, deauth injection, and man-in-the-middle attacks. It can also act as a fake AP.2. AutopsyAutopsy operates as a graphical front end to The Sleuth Kit, which is also included in the Kali package. The Sleuth Kit is able to search down into a hard disk and recover files that have been deleted or possibly damaged by the loss of the File Access Table.The combination of Autopsy and The Sleuth Kit is frequently used by law enforcement agencies to extract files from the confiscated devices of suspects. It is also able to extract images from phone memory cards.3. ArmitageArmitage is an attack manager that uses Metasploit as a back end. While the user is able to visualize discovered computers in Armitage, further commands in the interface get interpreted down to Metasploit, which implements further exploration.As well as identifying devices and documenting their software and services, Armitage provides a collaboration platform for teams working on a pen testing project. It also enables an attack strategy to be formulated and then implemented through Metasploit.4. Burp SuiteBurp Suite is available in free and paid versions you get the free Community Edition bundled in with Kali Linux. The Burp Suite version that comes with Kali is able to intercept the traffic that passes between a Web server and a Web browser to deliver and render a Web page.It is possible to force the transaction onto HTTP to prevent the use of encryption. The unprotected data passing over the network can then be scanned for important information, such as login credentials. You can read more about Burp Suite and how to use it in our Burp Suite Cheat Sheet.5. BeEFBeEF stands for the Browser Exploitation Framework. It is a Web application pen testing tool that tests sites loaded into a test browser and scan for exploits. BeEF works at the command line and then triggers the opening of a browser to run the tests.The system can be used to perform attack strategies that try to get into the supporting Web server through HTTP transactions.6. Cisco Global ExploiterThe Cisco Global Exploiter is not a Cisco product; rather, it specializes in hacking Cisco-produced routers and switches. Cisco devices are very widely used, and they have their own operating system, called IOS. The Cisco Global Exploiter is a command-line utility that attempts to break into a device, using default and commonly-used passwords for the administrator account.Sticking to a built-in knowledge of IOS, the Cisco Global Exploiter explores for known vulnerabilities with Cisco devices.7. EttercapEttercap is a packet capture tool that can facilitate a man-in-the-middle attack and also credentials capture. The system is available as a command-line utility and it also has a rudimentary graphical user interface.The Ettercap system uses ARP poisoning to establish a position as a listener between a Web server and a browser. It lets the attacker diver traffic from an intended destination and it is also able to use the system to create a fake AP to capture all traffic in an unencrypted format. You can find out more about Ettercap in our Ettercap Cheat Sheet.8. ForemostForemost operates at the command line and it performs data recovery functions. Foremost works on disks that might have been damaged, losing the FAT and scattering the links between segments containing parts of files. It is able to reassemble those fragments back into accessible files.This utility was created by agents of the US Air Force Office of Special Investigations and it is used by law enforcement agencies around the world for recovering deleted or damaged files, including images. It is also used for copying entire disks for later analysis.9. HashcatHashcat is a command-line utility that focuses on system passwords. It is able to crack passwords or, as the creators express it, to recover passwords. As its name implies, the system works on hashing algorithms. Many systems store passwords in a scrambled state; Hashcat tries to work out which algorithm was used for that protection and then tries to reverse it to reveal the passwords in plain text.10. HydraHydra, which is also known as THC Hydra, is a password cracker. Hydra works at the command line and it is notable for the speed of its password attacks. This is achieved by running several attempts simultaneously.The parallel operations of Hydra enable hackers and pen-testers to quickly cycle through a long list of possible authentication protocols until it works out exactly which system to use. It then performs a range of attack strategies to discover username and password combinations.11. John the RipperJohn the Ripper is another password cracker. This also detects the hashing algorithm in use and then tries to decrypt the password file. The John the Ripper package includes a range of password cracking tools, including brute force password guessing. You can choose to generate a password dictionary to try or import one from another tool. It is also possible to create your own dictionary to use for password guessing attempts.12. KismetKismet is a packet sniffer that can be used to explore a network. Where this tool is different from most network discovery tools, it works on wireless networks. Kismet has a great user interface that features live signal strength indicators for each channel.By identifying all channels, the system can capture traffic in a conversation. By examining the contents of transmission to discover new devices with their identities and user accounts. Kismet can also be used as an intrusion detection system.13. MaltegoMaltego is an unusual tool and can be very powerful. It constructs relationships between information points. The first task of the system is to discover devices, scan them, and document the software and settings of each. It then creates a map of these dependencies.The Maltego mapping system can also be applied to user accounts and hierarchies. One of the most powerful capabilities of Maltego is its ability to map social media accounts and the connections between them. Maltegos crawling can be limited to a specific network or allowed to chain out all over the world, passing through a range of systems.14. Metasploit Framework Metasploit is a well-known hacker tool that is owned and developed by the cybersecurity firm, Rapid7. There are two versions of Metasploit. The edition that is bundled into Kali, Metasploit Framework, is free. The higher version is a paid tool, called Metasploit Pro.The main purpose of Metasploit Framework is a vulnerability scanner. After a system sweep to discover exploits, Metasploit offers an interface in which to compose attacks.15. NiktoNikto is a web vulnerability scanner that runs at the command line. The tool looks for 6,700 dangerous programs and also scans services, such as Web server and email server systems it includes scans for a total of 1,250 server versions.After identifying all of the software on a Web server and categorizing it as threatening, weak, or worthwhile, the system then checks through all of the settings of those systems. The Nikto system can be used to protect a system by testing intrusion detection systems.16. NmapNmap, also called Network Mapper is a highly respected network discovery tool. This is a command-line tool that can also be run through scripts. For a GUI version, you should access Zenmap, which is also included with Kali Linux.Nmap operates as a packet sniffer. It looks into the headers of passing traffic to log all of the different devices and the applications operating on each that generate traffic.The facilities of Nmap are designed to run within a network. It can be used by network administrators or consultants who want to quickly document a network. It is also a very useful tool for white hat hackers.17. OWASP ZAPOWASP is the Open Web Application Security Project. One of the key products of OWASP is the Zed Attack Proxy (ZAP). The service is centered on a traffic interceptor that focuses on Web transactions. This system has a graphical user interface, which makes it easy to use.Tools within the ZAP system include a web crawler, a URL fuzzer, and a vulnerability scanner. These systems operate through a proxy server, which acts as a collection point for vulnerability data. These processes test the security services of a network and the Web server itself.18. sqlmapSqlmap is a command-line utility that offers a number of different ways to probe the security surrounding databases that work as services to websites and networked services, such as ERPs.The implementation of sqlmap is formed through one command, which can be modified by a very large number of options. Every run of this program performs a scan on a database that is accessed through a specific URL or a local address. The standard scan will identify the DBMS and then try to attack it with a range of SQL injection strategies.The sqlmap system can be used to document databases, crack credentials, and extract data. We examine this tool in greater detail in the sqlmap Cheat Sheet.19. WiresharkWireshark is a very widely-used packet sniffer and you probably already use it. This system is able to extract passing network packets on LANs and wireless networks even Bluetooth. The service provides a GUI interface and there is also a command-line version called TShark.You probably wont use Wireshark exclusively but it is likely to be your top choice for a packet sniffer among all of the alternatives included in the Kali Linux bundle. This system is able to exchange data with system management tools and analysis utilities, so it will form the data feed for many other applications in your armory.20. WPScanWordPress is very widely implemented and is the most popular content management system in the world. The service has its own environment, which can make it difficult for security tools to fully explore a WordPress-based website for vulnerabilities. WPScan specializes in uncovering vulnerabilities within WordPress implementations.The free version of WPScan, which is integrated into Kali Linux is a command-line system. This makes it a little harder to use for non-technical website owners. However, it is worth putting in the time to learn how to use this vulnerability scanner because it searches for more than 23,000 WP-specific exploits.Kali Linux FAQsKali Linux isnt designed as a tool for beginners. The core of the tool is the Linux operating system, so you need to know the Linux command set first of all. Many of the tools included in the Kali Linux package are command-line systems and require a lot of studying to use because they are not as user-friendly as applications that have a GUI interface.Ubuntu and Kali are two versions of Linux and both are derivatives of Debian. Kali has much more than Ubuntu because it comes packaged with a long list of cybersecurity tools. If you dont need those security tools, all of the features of Kali would be a waste of space on your computer, so you would be better off with Ubuntu.Kali Linux is not illegal. The bundle of tools included with it are meant for use by penetration testers. The purpose of penetration testing is to use the methods deployed by hackers in order to test the security of an IT system. In order to provide the systems needed for penetration testing, Kali Linux includes many of the tools used by hackers. So, the package could be put to harmful use.

Ethical hacking linux commands. Kali ethical hacking. Ethical hacking commands in kali linux.