Kali Linux

Cheat Sheet

LINUXSIMPLY

Information Gathering	
ACE-voip	Detect and analyze voice over IP traffic
Amap	Identify open ports and services on a remote system
APT2	Automatic penetration testing and renerating reports
arp-scan	Discover hosts on a network
Automater	Automatic OSINT gathering
bing-ip2hosts	Enumerate hostnames from Bing search result
braa	Detect and analyze broadcast radio signals
CaseFile	Create and manage threat intelligence reports
CDPSnarf	Extract CDP information from a network
copy-router-config	Backing up router configurations or transderring configurations to a new router
DMitry	Gather target network information including port scanning and WHOIS lookups
dnmap	Identify host and services on a network
dnsenum	Gather information about Dns records including subdomains
dnsmap	Identify active DNS servers and associated hostnames
DNSRecon	DNS reconnaissance tool to gather information about servers, zone transfer and IP addresses
dnstracer	Trace DNS queries to identify problems and misconfigurations
dnswalk	Check common DNS misconfiguration
DotDotPwn	Exploit directory traversal vulnerabilities
enum4linux	Gather information from Windows and Samba system including shares, users and passwords
enumIAX	Gather information from IAX-based VoIP systems
EyeWitness	Generate screenshots of web applications
Faraday	Manage and collaborate on vulnerabiity scans and security assessment
Fierce	Identify non-contiguous IP space and map network infrastructure
Firewalk	Determine specific traffic blocking by firewall and by analyzing TTl values

Vulnerability Analysis	
BBQSQL	A blind SQL injection and exploitation tool
BED	A network protocol fuzzing tool
cisco-global-exploiter	Exploit vulnerabilities in Cisco devices
cisco-ocs	Scan and exploit Cisco devices
cisco-torch	Test and scan the security of Cisco devices
copy-router-config	Back up and restore Cisco router configurations
Doona	Test the security of network devices and protocols
DotDotPwn	Exploit directory traversal vulnerabilities
HexorBase	A database management and exploitation tool
jSQL Injection	A SQL injection exploitation tool
Lynis	A security auditing and hardening tool for Linux and Unix-based systems
Nmap	Network exploration and security auditing tool
ohrwurm	A local root exploitation tool
openvas	A vulnerability scanner and management tool
Oscanner	Scan Oracle databases for vulnerabilities
Powerfuzzer	A web application fuzzing and discovery tool
sfuzz	A protocol fuzzer and and vulnerability scanner
SidGuesser	Identify valid user accounts in Windows domains
SIPArmyKnife	Test the security of VoIP systems
sqlmap	A SQL injection exploitation tool
Sqlninja	A SQL server injection and takeover tool
sqlsus	Identify and exploit SQL injection vulnerabilities
tnscmd10g	Test and exploit Oracle TNS Listener vulnerabilities
unix-privesc-check	Identify privilege escalation vulnerabilities in Unix-based systems

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

Kali Linux

Cheat Sheet

LINUXSIMPLY

fragroute/fragrouter	Intercept and modify network traffic at IP fragmentation level
Ghost Phisher	Security testing for phishing attacks
GoLismero	Web security testing tool
goofile	Search specific file types on a target domain
hping3	
ident-user-enum	Identify user accounts on systems that use the Ident protocol
InSpy	LinkedIn reconnaissance tool to gather information about employees, companies and job postings
InTrace	Trace the route of TCP packets through a network
iSMTP	Test the security of SMYP servers
lbd	Identify load balancers and web application firewalls
Maltego Teeth	Identify connections and relationships between entities
masscan	A fast port scanner used for vulnerability assessment
Metagoofil	Gather information and extract metadata from public documents
Miranda	Tool for exploiting UPnP devices
Metagoofil	Gather information and extract metadata from public documents
Nikto	Web server scanner
SMBMap	Enumerate and scan SMB shares
ntop	Network traffic monitoring and analysis
OSRFramework	Intelligence gathering framework used for data mining
p0f	Passive network traffic analysis for identidying the operating systems and applications used on networked devices
Parsero	Identify input validation related vulnerablities of web applications
SET	Tool for performing social engineering attacks, password attacks etc.
smtp-user-enum	Enumberate usernames on a target SMTP server
snmp-check	Enumerate and check the security of SNMP devices
SPARTA	Graphical interface for network infrastructure penetration testing
Yersinia	Network protocol analyzer and attack tool for testing network security

Wireless Attacks

Airbase-ng	Configure and attack wireless access points
Aircrack-ng	Audit and test wireless network
Airdecap-ng and Airdecloak-ng	Decrypt and deobfuscate captured wireless traffic
Aireplay-ng	Inject taffic to wireless networks to test their security
airgraph-ng	Generate graphs from wireless network data
Airmon-ng	Enable and Disable monitor mode on wireless interfaces
Airodump-ng	Capture wireless traffic and analyze it
airodump-ng-oui-update	Update the OUI databases used by airodump-ng
Airolib-ng	Manage and crack password hashes for WPA and WPA2
Airserv-ng	Run a wireless access point on a Linux system
Airtun-ng	Create encrypted tunnels over wireless networks
Asleap	Crack MS-CHAPv1 and MS-CHAPv2 authentication protocols
Besside-ng	Capture and crack WEP and WPA encrypted wireless traffic
Bluelog	Scan and log Bluetooth devices
BlueMaho	Discover and attack Bluetooth devices
Bluepot	Simulate Bluetooth honeypots to detect and track attackers
BlueRanger	Control Bluetooth devices remotely
Bluesnarfer	Exploit Bluetooth vulnerabilities and gaining unauthorized access to devices
Bully	Brute-forcing WPS pins to gain access to wireless networks
coWPAtty	Crack pre-shared keys for WPA-PSK networks
crackle	Crack encrypted Bluetooth traffic
eapmd5pass	Crack MD5 hashes of EAP passwords
Easside-ng	Crack WEP and WPA encrypted wireless traffic

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

Kali Linux

Cheat Sheet

LINUXSIMPLY

sslcaudit	Audit SSl/Tls certificates on a web server
SSLsplit	Intercept and decrypt SSL/TLS traffic
sslstrip	Tool for performing man in the middle attacks on SSL/TLS encrypted connections
SSLyze	Test SSL/TLS servers and clients
Sublist3r	Enumerate subdomains of a target domain using search engines
THC-IPV6	Attack and test IPv6 networks
theHarvester	Gather information of a target domain from various public sources
TLSSLed	Evaluate the security of SSL/TLS connections
twofi	Find potential usernames and passwords from Twitter
Unicornscan	A fast and powerful network scanning tool
URLCrazy	Generate and test domain typos and variations
Wireshark	Network protocol analyzer for capturing and analyzing network traffic
WOL-E	Tool for Wake-On-LAN attacks and network discovery
Xplico	Extract application data from network traffic

Forensics Tools

Binwalk	Analyze and extract firmware images
bulk-extractor	*Extract artifacts from binary files*
Capstone	A multi-platform, multi-architecture disassembly framework
chntpw	*Reset passwords on Windows systems*
Cuckoo	An automated malware analysis system
dc3dd	*A tool for imaging and wiping hard drives*
ddrescue	Rescuing data from damaged disks
DFF	*A forensic framework for analyzing digital evidence*
diStorm3	A disassembler library for x86/AMD64
Dumpzilla	*Analyze Mozilla browser history*

Fern Wifi Cracker	Audit and crack wireless networks
FreeRADIUS-WPE	Exploit weak credentials in the FreeRADIUS server
Ghost Phisher	Create phishing attacks on wireless networks
GISKismet	Map and analyze wireless networks using GPS data
Gqrx	A receiver for exploring wireless signals
gr-scan	scan and decode various radio signals
hostapd-wpe	Test and exploit the WPE feature in hostapd
ivstools	Convert and manipulate IVs for WEP cracking
kalibrate-rtl	Calibrate the frequency offset of RTL-SDR dongles
KillerBee	Explore and exploit ZigBee and IEEE 802.15.4 networks
Kismet	Detect and analyze wireless networks
makeivs-ng	Generate and inject fake IVs for WEP cracking
mdk3	Attack wireless networks by flooding them with deauthentication, disassociation, and other packets
mfcuk	Crack Mifare Classic RFID cards
mfoc	Crack Mifare Classic RFID cards
mfterm	Interact with RFID cards
Multimon-NG	Decode various radio signals
Packetforge-ng	Create and inject custom packets into wireless networks
PixieWPS	Exploit the WPS design flaw to recover WPA/WPA2 passwords
Pyrit	Perform advanced WPA/WPA2 password cracking using GPU power
Reaver	A tool for brute-forcing WPS
redfang	A Bluetooth scanner and vulnerability assessment tool
RTLSDR Scanner	A radio scanner for spectrum analysis and monitoring
Spooftooph	A tool for Bluetooth device spoofing and cloning
Tkiptun-ng	WPA encryption key recovery using TKIP vulnerabilities
Wesside-ng	Automated wirelss network hacking for WEP, WPA and WPA2 encryption

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

Kali Linux

Cheat Sheet

LINUXSIMPLY

extundelete	Recover deleted files from ext3/ext4 partitions
Foremost	*Extract files from disk images*
Galleta	Analyze browser cookies
Guymager	*Create forensic images*
iPhone Backup Analyzer	Analyze iPhone backups.
p0f	*A tool for passive OS fingerprinting and network analysis*
pdf-parser	A tool for analyzing PDF files
pdfid	*Analyze and detect malicious PDF files*
pdgmail	Analyze Gmail artifacts
peepdf	*Analyze and explor PDF files*
RegRipper	Analyze Windows registry hives
Volatility	*Analyze memory dumps*

Exploitation Tools	
Armitage	A graphical cyber attack management tool
Backdoor Factory	*Add backdoors to binaries*
BeEF	Penetration testing focuses on browser-based attacks
Commix	*A command injection exploitation tool*
crackle	Break Bluetooth Smart encryption
exploitdb	*A database of known exploits and vulnerable software*
jboss-autopwn	Exploit vulnerabilities in JBoss servers
MSFPC	*Create Metasploit payloads*
RouterSploit	*Test vulnerabilities in routers and other embedded devices*
ShellNoob	Generate shellcode and convert shellcode to assembly

Sniffing & Spoofing	
SIPp	Test and benchmark SIP-based VoIP systems
rtpbreak	Detect, reconstruct, and analyze RTP sessions
SIPVicious	Audit SIP-based VoIP systems
rtpmixsound	Mix audio into RTP streams

Wifi Honey	Perform honey spot attacks on wireless networks
wifiphisher	Steal credential of wireless network
Wifitap	Create virtual wireless access points and monitor network traffic
Wifite	Audit and attack automated wireless network
wpaclean	Filter and clean WPA/WPA2 handshake capture file

Hardware Hacking	
android-sdk	A software development kit for developing Android applications
Arduino	An open-source electronics platform for creating interactive projects
dex2jar	Convert Android DEX files to Java JAR files
Sakis3G	Connect to 3G mobile networks
smali	An assembler/disassembler for Android's dex format

Reverse Engineering	
apktool	Reverse engineer and modify Android APK files
diStorm3	A disassembler library used for binary analysis
edb-debugger	A cross-platform debugger for x86, ARM, MIPS, and PowerPC executables
jad	Analyze and reverse engineer Java bytecode
javasnoop	Intercept and analyze Java method calls
JD-GUI	Decompile and analyze Java bytecode
OllyDbg	A 32-bit assembler-level analyzing debugger
Valgrind	Debug and profile Linux programs
YARA	Match pattern and identify malware and other suspicious files

Web Applications	
apache-users	Find usernames on an Apache web server
Arachni	A feature-rich web application security scanner
BlindElephant	Identify web applications version number
Burp Suite	Web application testing framework
CutyCapt	Capture website screenshots
DAVTest	Test the security of WebDAV servers
DIRB	A tool used for web content discovery

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

Kali Linux

Cheat Sheet

LINUXSIMPLY

bettercap	A Swiss Army knife for network attacks and monitoring, including sniffing, spoofing, and MITM attacks
DNSChef	A DNS proxy that can be used to forge DNS responses and redirect traffic to malicious sites
fiked	A fake IKE daemon used for launching MITM attacks against IKEv1-encrypted connections
hamster-sidejack	Perform session hijacking attacks against web applications
HexInject	Craft and inject packets into a network
iSMTP	Test the security of SMTP servers by sending a large number of emails
isr-evilgrade	Exploit software vulnerabilities and perform automatic updates of malicious software
mitmproxy	A SSL-capable intercepting proxy used for intercepting, modifying, and replaying traffic between clients and servers
ohrwurm	Generate payloads and test the detection capabilities of antivirus software
protos-sip	Test the security of SIP-based VoIP systems
rebind	Perform DNS rebinding attacks against web applications
responder	Steal NTLMv1/v2 hashes and perform LLMNR/NBT-NS poisoning
rtpinsertsound	Insert audio into RTP streams
sctpscan	Perform SCTP network scanning and fingerprinting
SIPArmyKnife	A tool used for testing the security of SIP-based VoIP systems
SniffJoke	Manipulate network traffic in real-time
VoIPHopper	Detect and exploit VoIP security vulnerabilities
xspy	Monitor and analyze X11 traffic
zaproxy	Test security of web applications by scanning

deblaze	Discover hidden files and directories on a web server
DirBuster	A multi-threaded web application scanner
FunkLoad	A web functional testing and load testing tool
Gobuster	Brute forcing directories and files on web servers
Grabber	Detect security vulnerabilities of web applications
hURL	A tool used for web application testing and discovery
jboss-autopwn	Exploit vulnerable JBoss application servers
joomscan	Identify vulnerabilities in Joomla! CMS
PadBuster	Test Padding Oracle vulnerabilities in web applications
Paros	A web application testing proxy used to intercept and analyze web traffic
Parsero	A tool used for web application fingerprinting and directory discovery
plecost	A WordPress vulnerability scanner
Powerfuzzer	A highly automated web application vulnerability scanner
ProxyStrike	Attack web applications through proxies
Recon-ng	A web reconnaissance framework
Skipfish	A web application security scanner used for reconnaissance and discovery
ua-tester	Test user-agent strings in web applications
Uniscan	Security scanner used for finding vulnerabilities
w3af	A framework used for web application security testing
WebScarab	A Java-based web application testing proxy used for intercepting and analyzing web traffic
Webshag	A multi-threaded, multi-platform web application vulnerability scanner
WebSlayer	Find vulnerabilities in web applications

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

Kali Linux

Cheat Sheet

LINUXSIMPLY

Password Attacks	
BruteSpray	Automate password spraying attacks against multiple hosts simultaneously
CeWL	Generate custom wordlists for password cracking and other security assessments
chntpw	Reset passwords on Windows systems by modifying the Windows registry
CmosPwd	Recover CMOS passwords on Windows systems
creddump	Extract password hashes and other credentials from Windows systems
crowbar	Brute-force attacks against remote authentication services
crunch	Generate custom wordlists for password cracking and other security assessments
findmyhash	Identify the hash algorithm used to encrypt password hashes
gpp-decrypt	Decrypt Group Policy Preferences (GPP) passwords on Windows systems
hash-identifier	Identify the type of hash used to encrypt password hashes
Hashcat	A tool used for advanced password cracking and recovery
HexorBase	A tool used for database management and exploitation
THC-Hydra	Brute-force attacks against remote authentication services
John the Ripper	A tool used for password cracking and recovery
Johnny	A graphical user interface for John the Ripper password cracking tool
keimpx	Exploit vulnerabilities in Microsoft Windows systems
Maskprocessor	Generate custom wordlists based on specified criteria
Ncrack	Brute-force attacks against remote authentication services
oclgausscrack	Advanced password cracking and recovery on systems with OpenCL-compatible hardware
ophcrack	Password cracking and recovery on Windows systems
PACK	Advanced password cracking and recovery
WebSploit	A web application security testing framework
Wfuzz	A web application fuzzer used for brute forcing directories and files on web servers
WhatWeb	Fingerprint web servers and identify vulnerabilities
WPScan	A WordPress vulnerability scanner
XSSer	Find and exploit XSS vulnerabilities
fimap	Automate web application attacks and vulnerability scanning

Stress Testing	
DHCPig	Flood DHCP servers with requests, causing them to crash or become unavailable
iaxflood	Flood SIP servers with requests, causing them to crash or become unavailable
Inundator	Flood a network with random packets, causing network congestion and slowdowns
inviteflood	*Flood SIP servers with INVITE requests, causing them to crash or become unavailable*
ipv6-toolkit	Collection of tools for testing and exploiting IPv6 networks
rtpflood	*Flood VoIP servers with RTP packets, causing them to crash or become unavailable*
SlowHTTPTest	Test the vulnerability of web servers to Slow HTTP
t50	Generate network traffic and test the performance of network devices under heavy loads
Termineter	Test the security of Smart Grid devices and protocols
THC-SSL-DOS	Flood SSL servers with SSL handshake requests, causing them to crash or become unavailable

Maintaining Access	
CryptCat	Create encrypted and authenticated connections between two hosts
Cymothoa	Inject shellcode into a running process in order to gain remote access

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet

patator	*Brute-force attacks against multiple protocols and services*
phrasendrescher	*Generate custom wordlists based on natural language patterns*
polenum	*Retrieve password policy information from Windows systems*
RainbowCrack	*Advanced password cracking and recovery using rainbow tables*
SecLists	*A collection of various security-related wordlists for password cracking and other security assessments*
SQLdict	*Generate custom wordlists based on SQL queries*
Statsprocessor	*Generate custom wordlists based on statistical analysis of existing passwords*
THC-pptp-bruter	*Brute-force attacks against PPTP VPNs*
TrueCrack	*A tool used for advanced password cracking and recovery*
wordlists	*Collection of various wordlists for password cracking*

Reporting Tools

CaseFile	Create diagrams and charts to aid in the organization and visualization of data during investigations
cherrytree	A hierarchical note-taking application that allows the creation and organization of notes and code snippets
CutyCapt	Capture screenshots of web pages from the command line
dos2unix	Convert DOS-style line endings to Unix-style line endings in text files
Dradis	A collaboration and reporting platform for security testing professionals
MagicTree	Visualize and analyze data from different sources, such as file systems, network traffic, and databases
Nipper-ng	A tool used for auditing network device security configurations
pipal	A password analyzer and cracking tool used to identify weak passwords
RDPY	Perform remote desktop protocol operations, such as screen capture and input injection

dbd	*A backdoor daemon that allows remote access to a system via a network connection*
dns2tcp	*A tool used to tunnel TCP traffic over DNS protocols*
HTTPTunnel	*A tool used to tunnel traffic over HTTP protocols*
Intersect	*Generate payloads for exploitation of vulnerabilities*
Nishang	*Create and execute PowerShell scripts for penetration testing*
PowerSploit	*Collection of PowerShell scripts for penetration testing and other security assessments*
pwnat	*Bypass NAT firewalls and establish direct connections between two hosts*
RidEnum	*Enumerate user accounts and groups on Windows systems*
sbd	*Create a secure backdoor connection between two hosts*
shellter	*Bypass antivirus software and other security mechanisms*
U3-Pwn	*Exploit security vulnerabilities in U3 USB smart drives*
Webshells	*Collection of scripts and tools used for remote access and exploitation of web servers*
Weevely	*A webshell used to gain remote access to web servers and execute commands*
Winexe	*Remotely execute commands on Windows systems from a Linux or Unix host*

Prepared By: *Md Zahidul Islam Laku*

Web: Kali Linux Cheat Sheet