Tools

Cybersecurity Careers and Studies (NICCS)

https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool

The following are use cases for penetration testing tools:

Reconnaissance
Enumeration
Vulnerability scanning
Credential attacks
Persistence
Configuration compliance
Evasion
Decompilation
Forensics
Debugging
Software assurance (including fuzzing, static application security testing [SAST], and dynamic application security testing [DAST])

Penetration Testing - Focused Linux Distributions
Several Linux distributions include numerous penetration testing tools. The purpose of these Linux distributions is to make it easier for individuals to get started with penetration testing, without having to worry about software dependencies and compatibility issues that could be introduced when installing and deploying such tools. The following are the most popular penetration testing Linux distributions:

Kali Linux : https://www.kali.org/
Parrot OS : https://parrotsec.org/
BlackArch Linux : https://blackarch.org/

Ethical Hacker Kali Linux: Virtual Machine for the Ethical Hacker course
https://skillsforall.com/resources/lab-downloads?courseLang=en-US

The following sections cover the tools that are most commonly used in penetration testing engagements.

Common Tools for Reconnaissance and Enumeration

Tools for Passive Reconnaissance
Passive reconnaissance involves attempting to gather information about a victim by using public information and records but not using any active tools like scanners or sending any packets to the victim.
The industry often refers to publicly available information as open-source intelligence (OSINT). https://osintframework.com/

```
$ nslookup store.h4cker.org
$ dig store.h4cker.org
$ host store.h4cker.org
$ whois h4cker.org
```

FOCA
Fingerprinting Organization with Collected Archives (FOCA) is a tool designed to find metadata and hidden information in documents. FOCA can analyze websites as well as Microsoft Office, Open Office, PDF, and other documents. You can download FOCA from https://github.com/ElevenPaths/FOCA FOCA analyzes files by extracting EXIF (exchangeable image file format) information from graphics files, as well as information discovered through the URL of a scanned website.

ExifTool
Popular tool for extracting EXIF information from images. EXIF is a standard that defines the formats for images, sound, and ancillary tags used by digital equipment such as digital cameras, mobile phones, and tablets. You can download ExifTool from https://exiftool.org

Ex:
$ exif some_pic.jpg

theHarvester
Tool that can be used to enumerate DNS information about a given hostname or IP address. It can query several data sources, including Baidu, Google, LinkedIn, public Pretty Good Privacy (PGP) servers, Twitter, vhost, Virus Total, ThreatCrowd, CRT.SH, Netcraft, and Yahoo.

Ex:
$ theHarvester -d website.com -l 500 -b all

Shodan
Search engine for devices connected to the Internet. Shodan continuously scans the Internet and exposes its results to users via its website (https:// www.shodan.io) and via an API. Attackers can use this tool to identify vulnerable and exposed systems on the Internet (for example, misconfigured IoT devices, infrastructure devices). Penetration testers can use this tool to gather information about potentially vulnerable systems exposed to the Internet without actively scanning their victims. Figure 10-5 shows the results of a Shodan search for Cisco Smart Install client devices exposed to the Internet.

Maltego
Gathers information from public records, is one of the most popular tools for passive reconnaissance. It supports numerous third-party integrations. There are several versions of Maltego, including a community edition (which is free) and several commercial Maltego client and server options. You can download and obtain more information about Maltego from https://www.paterva.com Maltego can be used to find information about companies, individuals, gangs, educational institutions, political movement groups, religious groups, and so on. Maltego organizes query entities within the Entity Palette, and the search options are called “transforms.”

Recon-ng
Menu-based tool that can be used to automate the information gathering of OSINT. Recon-ng comes with Kali Linux and several other penetration testing Linux distributions, and it can be downloaded from https://github.com/lanmaster53/recon-ng

You can learn about all the Recon-ng options and commands at https://hackertarget.com/recon-ng-tutorial/

Censys
Tool developed by researchers at the University of Michigan, can be used for passive reconnaissance to find information about devices and networks on the Internet. It can be accessed at https://censys.io Censys provides a free web and API access plan that limits the number of queries a user can perform. It also provides several other paid plans that allow for premium support and additional queries.

Tools for Active Reconnaissance

Nmap

The enumeration of hosts is one of the first tasks that needs to be performed in active reconnaissance. Host enumeration could be performed in an internal network and externally (sourced from the Internet). When performed externally, you typically want to limit the IP addresses that you are scanning to just the ones that are part of the scope of the test. Doing so reduces the chances of inadvertently scanning an IP address that you are not authorized to test.

When performing an internal host enumeration, you typically scan the full subnet or subnets of IP addresses being used by the target. Example below shows a quick Nmap scan being performed to enumerate all hosts in the 192.168.0.0/24 subnet and any TCP ports they may have open. For additional information about the default ports that Nmap scans, see https://nmap.org/book/man-port-specification.html.

Ex: # nmap 192.168.0.0/24

Enum4linux

Great tool for enumerating SMB shares, vulnerable Samba implementations, and corresponding users.

Ex: # enum4linux -v 192.168.0.10

Common Tools for Vulnerability Scanning

There are numerous vulnerability scanning tools, including open-source and commercial vulnerability scanners, as well as cloud-based services and tools. The following are some of the most popular vulnerability scanners:

OpenVAS
Nessus
Nexpose
Qualys
SQLmap
Nikto
OWASP Zed Attack Proxy (ZAP)
w3af
DirBuster
Brakeman
Open Security Content Automation Protocol (SCAP) scanners
Wapiti
Scout Suite
WPScan (Wordpress scanner)

OpenVAS

Open-source vulnerability scanner that was created by Greenbone Networks. The OpenVAS framework includes several services and tools that enable you to perform detailed vulnerability scanning against hosts and networks.

OpenVAS can be downloaded from https://www.openvas.org, and the documentation can be accessed at https://docs.greenbone.net/#user_documentation

GVM-Kali (Greenbone Vulnerability Management)

https://www.kali.org/tools/gvm/

$ sudo apt install gvm

$ sudo gvm-check-setup -h
$ sudo greenbone-feed-sync --type nvt
$ sudo gvm-setup -h
$ sudo gvm-start
$ sudo gvm-stop

A browser window will open with a security warning that can be ignored. If the browser does not automatically open, start your browser manually and navigate to https://127.0.0.1:9392. Click the Advanced button and scroll down and accept the risk on the warning screen to proceed.

ou can easily start a scan in OpenVAS by navigating to Scans -> Tasks and selecting either Task Wizard or Advanced Task Wizard. You can also manually configure a scan by creating a new task.

Nessus
Vulnerability scanner from Tenable has several features that allow you to perform continuous monitoring and compliance analysis. Nessus can be downloaded from https://www.tenable.com/downloads/nessus

Version Free for Education
https://www.tenable.com/products/nessus/nessus-essentials

Tenable also has a cloud-based solution called Tenable.io. For information about Tenable.io, see https://www.tenable.com/products/tenable-io

Qualys
Is a security company that created one of the most popular vulnerability scanners in the industry. It also has a cloud-based service that performs continuous monitoring, vulnerability management, and compliance checking. This cloud solution interacts with cloud agents, virtual scanners, scanner appliances, and Internet scanners.

Information about the Qualys scanner and cloud platform can be accessed at https://www.qualys.com

SQLmap
Is often considered a web vulnerability and SQL injection tool. It helps automate the enumeration of vulnerable applications, as well as the exploitation of SQL injection techniques that you learned in Module 6, “Exploiting Application-Based Vulnerabilities.” You can download SQLmap from http://sqlmap.org

You can practice your penetration testing skills by using tools such as SQLmap against vulnerable applications. The Art of Hacking GitHub repository includes a list of vulnerable servers and applications that you can download and use to practice your skills in a safe environment; see https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/vulnerable_servers

Nikto
Popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

$ nikto --help
$ nikto -dbcheck
$ nikto -h http://scanme.nmap.org
$ nikto -h https://nmap.org -ssl
$ nikto -h <IP Address Target> -o website-scan.htm -Format html
# nmap -p 80 10.1.1.0/24 -oG - | nikto -h

OWASP Zed Attack Proxy (ZAP)
According to OWASP, OWASP Zed Attack Proxy (ZAP) “is one of the world’s most popular free security tools and is actively maintained by hundreds of international volunteers.” Many offensive and defensive security engineers around the world use ZAP, which not only provides web vulnerability scanning capabilities but also can be used as a sophisticated web proxy. ZAP comes with an API and also can be used as a fuzzer. You can download and obtain more information about OWASP ZAP from https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

w3af
Another popular open-source web application vulnerability scanner is w3af. w3af can be downloaded from https://w3af.org, and its documentation can be obtained from https://w3af.org/howtos

For detailed w3af usage and customization, refer to https://docs.w3af.org/en/latest

DirBuster
Tool that was designed to brute force directory names and filenames on web application servers. DirBuster is currently an inactive project, and its functionality has been integrated into and enhanced in OWASP ZAP as an add-on.

Ex:

Gobuster

Common Tools for Credential Attacks

The following are some of the most popular tools that can be used to brute force, crack, and compromise user credentials:

John the Ripper
Cain and Abel
Hashcat
Hydra
RainbowCrack
Medusa and Ncrack
CeWL
Mimikatz
Patator

John the Ripper
Very popular tool for offline password cracking. John the Ripper (or john for short) can use search patterns as well as password files (or wordlists) to crack passwords. It supports different cracking modes and understands many ciphertext formats, including several DES variants, MD5, and Blowfish. John the Ripper does not support AES and SHA-2. To list the supported formats, you can use the john --list=formats command, John the Ripper can also be used to extract Kerberos AFS and Windows passwords. John the Ripper can be downloaded from https://www.openwall.com/john

```
$ john --list=formats
# adduser -m user1
# adduser -m user2
# adduser -m user3
# cat /etc/shadow | egrep "user1|user2|user3" > hashes.txt
# cat hashes.txt
# john hashes.txt
# john -show hashes.txt
```

Wordlists
One of the most popular wordlists is the rockyou wordlist, which includes thousands of passwords that have been exposed in real-world breaches. In addition, the following two sites have comprehensive lists of wordlists containing millions of passwords: https://www.openwall.com/wordlists and https://github.com/berzerk0/Probable-Wordlists

locate wordlist

Ex:
john --wordlist common.txt hashes.txt

The following website provides tutorials showing different use cases for John the Ripper: https://openwall.info/wiki/john/tutorials

Hashcat
Another password-cracking tool that is very popular among pen testers. It allows you to use graphical processing units (GPUs) to accelerate the password-cracking process.

Hashcat comes with Kali Linux and other penetration testing Linux distributions. You can also download it from https://hashcat.net/hashcat

Ex: Cracking Passwords with Hashcat
hashcat --force -m 0 -a 0 -o crack_pass.txt hashes.txt common.txt

Hydra
Another tool that can be used to guess and crack credentials. Hydra is typically used to interact with a victim server (for example, web server, FTP server, SSH server, file server) and try a list of username/password combinations.

Ex:

Medusa and Ncrack
Similar to Hydra, can be used to perform brute-force credential attacks against a system. You can install Medusa by using the apt install medusa command in a Debian-based Linux system (such as Ubuntu, Kali Linux, or Parrot OS). You can download Ncrack from https://nmap.org/ncrack or install it by using the apt install ncrack command.

Ex:
ncrack -p 22 --user chris -P my_list 172.18.104.166
medusa -u chris -P my_list -h 172.18.104.166 -M ssh

CeWL
Great tool that can be used to create wordlists. You can use CeWL to crawl websites and retrieve words. Example 10-38 shows how to use CeWL to create the wordlist words.txt by crawling the website https://theartofhacking.org You can download CeWL from https://digi.ninja/projects/cewl.php

Ex:
cewl -d 2 -m 5 -w words.txt https://theartofhacking.org

Mimikatz
Tool that many penetration testers and attackers (and even malware) use for retrieving password hashes from memory. It is also a useful post-exploitation tool. The Mimikatz tool can be downloaded from https://github.com/gentilkiwi/mimikatz Metasploit also includes Mimikatz as a Meterpreter

script to facilitate exploitation without the need to upload any files to the disk of the compromised host. You can obtain more information about the Mimikatz and Metasploit integration at https://www.offsec.com/metasploit-unleashed/mimikatz/

RainbowCrack
Attackers can use rainbow tables – precomputed tables for reversing cryptographic hash functions – to accelerate password cracking. It is possible to use a rainbow table to derive a password by looking at the hashed value.
The tool RainbowCrack can be used to automate the cracking of passwords using rainbow tables. You can download RainbowCrack from
http://project-rainbowcrack.com

The following website includes a list of rainbow tables that can be used with RainbowCrack: http://project-rainbowcrack.com/table.htm

Patator
Another tool that can be used for brute-force attacks on enumerations of SNMPv3 usernames, VPN passwords, and other types of credential attacks. You can download Patator from https://github.com/lanjelot/patator

Common Tools for Persistence

Netcat

PowerSploit is a collection of PowerShell modules that can be used for post- exploitation and other phases of an assessment. PowerSploit can be downloaded from https://github.com/PowerShellMafia/PowerSploit

Empire is a PowerShell-based post-exploitation framework that is very popular among pen testers. Empire is an open-source framework that includes a PowerShell Windows agent and a Python Linux agent. You can download Empire from https://github.com/EmpireProject/Empire

Common Tools for Evasion
In a pen testing engagement, you typically want to maintain stealth and try to evade and circumvent any security controls that the organization may have in place. Several tools and techniques can be used for evasion, including the following:

Veil
Tor
Proxychains
Encryption (SSL/TLS, VPN)
Encapsulation and tunneling using DNS and protocols such as NTP

Veil is a framework that can be used with Metasploit to evade antivirus checks and other security controls. You can download Veil from https://github.com/Veil-Framework/Veil and obtain detailed documentation from https://www.veil-framework.com

Ex:
veil
Select 1 Evasion
Veil/Evasion>: list
Veil/Evasion>:

Become Secure and Anonymous (VPN, TOR, Proxys)

Stealth Active Recon TOR+Proxychains (Anonymizing)

Install TOR Proxychains
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install -y tor proxychains
$ sudo apt autoremove

Configure Proxychains
$sudo vi /etc/proxychains4.conf
...
dynamic_chain
#strict_chain
...
defaults set to "tor"
#socket4 127.0.0.1 9050
socks5 127.0.0.1 9050

Start TOR Service
$ sudo systemctl start tor
$ systemctl status tor
$ curl ipinfo.io
$ proxychains curl ipinfo.io

Init Firefox via Proxychains
$ proxychains firefox https://bgp.he.net/
$ proxychains4 firefox https://whatismyipaddress.com

#Browsers TOR/Brave
https://www.torproject.org/download/

https://brave.com/pt-br/

https://www.dnsleaktest.com/

#Search Leaks via TOR
http://pwndb2am4tzkvold.onion/

#Proton Mail
https://proton.me/pt-br/mail

#OpenVPN Account Free

https://www.vpnbook.com/

https://openvpn.net/community-downloads/

# Install and configure OpenVPN
$ sudo apt -y install openvpn
$ sudo openvpn --client --config /home/dir-files/file.ovpn
$ curl ipinfo.io

Proxys
https://hidemy.io/en/proxy-list/

Exploitation Frameworks

Metasploit is by far the most popular exploitation framework in the industry. It was created by a security researcher named H. D. Moore and then sold to Rapid7. There are two versions of Metasploit: a community (free) edition and a professional edition. Metasploit, which is written in Ruby, has a robust architecture. Metasploit is installed in /usr/share/metasploit-framework by default in Kali Linux. All corresponding files, modules, documentation, and scripts are located in that folder.

ls /usr/share/metasploit-framework/documentation/

Metasploit has several modules:

auxiliary
encoders
exploits
nops
payloads
post (for post-exploitation)

You can launch the Metasploit console by using the msfconsole command.

Ex: Let's take a look at how to use an exploit against a vulnerable Linux server against a vulnerable IRC server
msfconsole
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.0.10
RHOST => 192.168.0.10
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
meterpreter> getsystem
meterpreter> hashdump

A free and detailed Metasploit training course can be obtained from https://www.offensive-security.com/metasploit-unleashed This course goes over each and every option in Metasploit and its architecture. I recommend you navigate throughout the options and become familiar with other modules, such as msfvenom, msf-pattern_create, msf-pattern_offset, and msf-metasm_shell.

The Metasploit framework allows you to create your own scripts, exploits, and post-exploitation Meterpreter scripts. These scripts are written in Ruby and located in the main Metasploit directory, scripts/meterpreter. You can see the source code for existing Metasploit scripts at https://github.com/rapid7/metasploit-framework/tree/master/scripts/meterpreter.

BeEF is an exploitation framework for web application testing. BeEF exploits browser vulnerabilities and interacts with one or more web browsers to launch directed command modules. Each browser can be configured in a different security context. BeEF allows you to launch a set of unique attack vectors and select specific modules in real time to target each browser and context.

You can download BeEF and obtain its documentation from https://beefproject.com

BeEF contains numerous command modules and uses a robust API that allows security professionals to quickly develop custom modules.

Common Decompilation, Disassembly, and Debugging Tools

Now let's cover some of the most popular decompilation, disassembly, and debugging tools in the industry.

The GNU Project Debugger (GDB)
Windows Debugger
OllyDbg
edb Debugger
Immunity Debugger
Interactive Disassembler (IDA)
Objdump

The GNU Project Debugger

The GNU Project Debugger (GDB) is one of the most popular debuggers among software developers and security professionals. With a debugger like GDB, you can troubleshoot and find software bugs, understand what a program was doing at the moment it crashed, make a program stop on specified conditions, and modify elements of a program to experiment or to correct problems.

Traditionally, GDB has mainly been used to debug programs written in C and C++; however, several other programming languages – such as Go, Objective-C, and OpenCL C – are also supported.

NOTE For a complete list of supported programming languages, go to https://www.gnu.org/software/gdb.

Example 10-43 shows a simple example of how GDB is used to debug and run a vulnerable application (vuln_program) written in C.

The run command is used to run an application inside GDB. The program executes and asks you to enter some text. In this example, a large number of A characters are entered, and the program exits. When the continue GDB command is executed, the text “Program terminated with signal SIGSEGV, Segmentation fault” is displayed. This indicates a potential buffer overflow (which is the case in Example 10-43).

Example 10-43 - Using GDB to Debug a Vulnerable Application

NOTE The source code for the vulnerable application in Example 10-43 is available at https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/buffer_overflow_example.

Ex:
gdb vuln_program

NOTE The website https://www.cprogramming.com/gdb.html includes additional examples of how to use GDB for debugging applications.

Windows Debugger

You can use the Windows Debugger (WinDbg) to debug kernel and user mode code. You can also use it to analyze crash dumps and to analyze the CPU registers as code executes. You can get debugging tools from Microsoft via the following methods:

By downloading and installing the Windows Driver Kit (WDK)
As a standalone tool set
By downloading the Windows Software Development Kit (SDK)

By downloading Microsoft Visual Studio
TIP Refer to the “Getting Started with Windows Debugging Microsoft” whitepaper to learn how to use WinDbg and related tools; see https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/getting-started-with-windows-debugging
You can obtain additional information about Windows debugging and symbols from https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/symbols

Immunity Debugger

Immunity Debugger is very popular among penetration testers and security researchers. It allows you to write exploits, analyze malware, and reverse engineer binary files. It supports a Python-based API. You can download Immunity Debugger from https://www.immunityinc.com/products/debugger/.

Common Tools for Forensics

The following are a few examples of tools and Linux distributions that can be used for forensics:

ADIA (Appliance for Digital Investigation and Analysis): ADIA is a VMware-based appliance used for digital investigation and acquisition that is built entirely from public domain software. Among the tools contained in ADIA are Autopsy, the Sleuth Kit, the Digital Forensics Framework, log2timeline, Xplico, and Wireshark. Most of the system maintenance uses Webmin. ADIA is designed for small to medium-sized digital investigations and acquisitions. The appliance runs under Linux, Windows, and macOS. Both i386 (32-bit) and x86_64 (64-bit) versions are available. You can download ADIA from https://forensics.cert.org/#ADIA.

CAINE: The Computer Aided Investigative Environment (CAINE) contains numerous tools that help investigators with analyses, including forensic evidence collection. You can download CAINE from http://www.caine-live.net/index.html.

Skadi: This all-in-one solution to parsing collected data makes the data easily searchable with built-in common searches and enables searching of single and multiple hosts simultaneously. You can download Skadi from https://github.com/orlikoski/Skadi.

PALADIN: PALADIN is a modified Linux distribution for performing various evidence collection tasks in a forensically sound manner. It includes many open source forensics tools. You can download PALADIN from https://sumuri.com/software/paladin/.

Security Onion: Security Onion, a Linux distro aimed at network security monitoring, features advanced analysis tools, some of which can help in forensic investigations. You can download Security Onion from https://github.com/Security-Onion-Solutions/security-onion.

SIFT Workstation: The SANS Investigative Forensic Toolkit (SIFT) Workstation demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques to intrusions can be accomplished using cutting-edge open source tools that are freely available and frequently updated. You can download SIFT Workstation from https://digital-forensics.sans.org/community/downloads.

NOTE The Art of Hacking GitHub repository includes a list of numerous tools that can be used for forensics: https://github.com/The-Art-of-Hacking/art-of-hacking/tree/master/dfir

Common Tools for Software Assurance

SpotBugs, Findsecbugs, and SonarQube

SpotBugs (previously known as Findbugs) is a static analysis tool designed to find bugs in applications created in the Java programming language. You can download and obtain more information about SpotBugs at https://spotbugs.github.io.
Findsecbugs is another tool designed to find bugs in applications created in the Java programming language. It can be used with continuous integration systems such as Jenkins and SonarQube. Findsecbugs provides support for popular Java frameworks, including Spring-MCV, Apache Struts, and Tapestry. You can download and obtain more information about Findbugs at https://find-sec-bugs.github.io.
SonarQube is a tool that can be used to find vulnerabilities in code, and it provides support for continuous integration and DevOps environments. You can obtain additional information about SonarQube at https://www.sonarqube.org.

Fuzzers and Fuzz Testing

Fuzz testing, or fuzzing , is a technique that can be used to find software errors (or bugs) and security vulnerabilities in applications, operating systems, infrastructure devices, IoT devices, and other computing device. Fuzzing involves sending random data to the unit being tested in order to find input validation issues, program failures, buffer overflows, and other flaws. Tools that are used to perform fuzzing are referred to as fuzzers. Examples of popular fuzzers are Peach, Mutiny Fuzzing Framework, and American Fuzzy Lop.

Peach

Peach is one of the most popular fuzzers in the industry. There is a free (open-source) version, the Peach Fuzzer Community Edition, and a commercial version. You can download the Peach Fuzzer Community Edition and obtain additional information about the commercial version at https://osdn.net/projects/sfnet_peachfuzz/releases/.

Mutiny Fuzzing Framework

The Mutiny Fuzzing Framework is an open-source fuzzer created by Cisco. It works by replaying packet capture files (pcaps) through a mutational fuzzer. You can download and obtain more information about Mutiny Fuzzing Framework at https://github.com/Cisco-Talos/mutiny-fuzzer.

NOTE The Mutiny Fuzzing Framework uses Radamsa to perform mutations. Radamsa is a tool that can be used to generate test cases for fuzzers. You can download and obtain additional information about Radamsa at https://gitlab.com/akihe/radamsa.

American Fuzzy Lop

American Fuzzy Lop (AFL) is a tool that provides features of compile-time instrumentation and genetic algorithms to automatically improve the functional coverage of fuzzing test cases. You can obtain information about AFL from https://lcamtuf.coredump.cx/afl/

Wireless Tools

The following are several wireless hacking tools that can help in testing wireless networks:

Wifite2: This is a Python program to test wireless networks that can be downloaded from https://github.com/derv82/wifite2

Rogue access points: You can easily create rogue access points by using open-source tools such

as hostapd. Omar Santos has a description of how to build your own wireless hacking lab and use hostapd at https://github.com/The-Art-of-Hacking/h4cker/blob/master/wireless_resources/virtual_adapters.md

EAPHammer: This tool, which you can use to perform evil twin attacks, can be downloaded from https://github.com/s0lst1c3/eaphammer.
mdk4: This tool is used to perform fuzzing, IDS evasions, and other wireless attacks. mdk4 can be downloaded from https://github.com/aircrack-ng/mdk4

Spooftooph: This tool is used to spoof and clone Bluetooth devices. It can be downloaded from https://gitlab.com/kalilinux/packages/spooftooph

Reaver: This tool is used to perform brute-force attacks against Wi-Fi Protected Setup (WPS) implementations. Reaver can be downloaded from https://gitlab.com/kalilinux/packages/reaver

Wireless Geographic Logging Engine (WiGLE): You can learn about this war driving tool at https://wigle.net

Fern Wi-Fi Cracker: This tool is used to perform different attacks against wireless networks, including cracking WEP, WPA, and WPS keys. You can download Fern Wi-Fi Cracker from https://gitlab.com/kalilinux/packages/fern-wifi-cracker.

Steganography Tools

Steganography is the act of hiding information in images, videos, and other files. You also learned about tools such as steghide.

The following are a few additional tools that can be used to perform steganography:

OpenStego: You can download this steganography tool from https://www.openstego.com

snow: This is a text-based steganography tool that can be downloaded from https://github.com/mattkwan-zz/snow

Coagula: This program, which can be used to make sound from an image, can be downloaded from https://www.abc.se/~re/Coagula/Coagula.html

Sonic Visualiser: This tool can be used to analyze embedded information in music or audio recordings. It can be downloaded from https://www.sonicvisualiser.org

TinEye: This is a reverse image search website at https://tineye.com

metagoofil: This tool can be used to extract metadata information from documents and images. You can download metagoofil from https://github.com/laramies/metagoofil

Cloud Tools

ScoutSuite: This collection of tools can be used to reveal vulnerabilities in AWS, Azure, Google Cloud Platform, and other cloud platforms. You can download ScoutSuite from https://github.com/nccgroup/ScoutSuite

CloudBrute: You can download this cloud enumeration tool from https://github.com/0xsha/CloudBrute

Pacu: This is a framework for AWS exploitation that can be downloaded from https://github.com/RhinoSecurityLabs/pacu

Cloud Custodian: This cloud security, governance, and management tool can be downloaded from https://cloudcustodian.io