Information Gathering

Tool: Maltego

Purpose	This is a program that is used to create a relational diagram(s) which are used to deliver a “threat picture” of the environment.
command line or graphical?	Graphical.
Requirements for usage	You need to register for an account as well as agree to the licencing agreement. Afterwards the application runs similarly to DIA
Creator	Paterva

Tool: legion

Purpose	Used as a semiautomated network penetration testing framework.
command line or graphical?	Graphical.
Requirements for usage	You must add a target machine as well as its host IP
Creator	GoVanguard

Vulnerability Analysis

Tool: nikto

Purpose	The purpose of nikto is to scan web servers for issues, outdated software, as well as any possible dangerous files.
command line or graphical?	Command line.
Requirements for usage	nikto follows shell syntax within the command line, and should be used with the following syntax: `nikto -CommandName`
Creator	Chris Sullo

Tool: afl

Purpose	Afl is a brute force style program used for fuzzing.
command line or graphical?	Command line.

Requirements for usage	You must compile programs using the afl compiler. While running afl within the console, it can take input test file and output file directories.
	To run the compiler:
	`afl-gcc -o program.c`
	To run the fuzz:
	`sudo afl-fuzz -i`

Creator	Michal Zalewski

Web Application Analysis

Tool: skipfish

Purpose	To create reports generated from probing security checks on a target machine.
command line or graphical?	Command line
Requirements for usage	Must follow shell syntax. To use within the terminal, the following must occur within the command: `skipfish -Authentication[optional] -CrawlScope -o outputDirectory URLofTarget`
Creator	Google Inc, Michal Zalewski, Niels Heinen, Sebastian Roschke

Tool: ZAP

Purpose	Used as a tool to detect vulnerabilities on applications and web servers.
command line or graphical?	Graphical.
Requirements for usage	You must choose if you would like to persist your current session. Opting out means that your data will not be saved once the program exits. You must have the url of the web application you would like to attack, as well as permission to attack the site.
Creator	OWASP.org

Database Assessment

Tool: sqlmap

Purpose	Used for penetration testing against SQL servers: detecting and exploiting any possible flaws.
command line or graphical?	Command line.
Requirements for usage	You need to have Python3 installed for sqlmap to work. You should also have permission to access the database though this method. You need sqlmap.py for this program to work as well. This can be cloned from this repository: https://github.com/sqlmapproject/sqlmap To run SQLmap within the command line: `python sqlmap.py -u “URLofTarget”`
Creator	Bernardo Damele Assumpcao Guimaraes, Miroslav Stampar

Tool: SQLite database browser

Purpose	Used to create, modify, and design sql files within the database.
command line or graphical?	Graphical
Requirements for usage	We must import the database from an sql file. The sql file MUST have the following line of code for it to be compatible with SQLite: `BEGIN TRANSACTION;`
Creator	Mauricio Piacentini

Password Attacks

Tool: john

Purpose	John is an optimized software used for cracking passwords.
command line or graphical?	Command line.
Requirements for usage	You must have a wordlist file to use against the hashed password file. Password files must be in the correct format for john or john modules.
Creator	Solar Designer

Tool: ncrack

Purpose	Ncrack is used to test networks/ devices within the network for weak passwords.
command line or graphical?	Command line.
Requirements for usage	You must have a list of IP addresses within the network, passwords, as well as the username of a user.
Creator	Insecure.Com LLC

Wireless Attacks

Tool: reaver

Purpose	Reaver is used to attack any Wifi Protected Setup.
command line or graphical?	Command line.

Requirements for usage	You must first scan for wifi networks using wash. Wash requires you to know the monitor mode as well as the channel. Using the access point given through the scan, you would then be able to use Reaver.
	How to scan using wash:
	`wash -i NameOfMonitorMode -c Channel -C`
	Reaver usage
	`reaver -i NameOfMonitorMode -b AccessPoint -v`

Creator	Tactical Network Solutions, Craig Heffner

Tool: fern wifi cracker

Purpose	Fern wifi cracker is used to crack and recover keys, as well as run network based attacks on internet connections (ethernet or wireless.)
command line or graphical?	Graphical
Requirements for usage	You must have Python 3 installed, as well as the Python Qt GUI library.
Creator	Saviour Emmanuel Ekiko

Reverse Engineering

Tool: clang

Purpose	Clang is a c compiler used for static analysis.
command line or graphical?	Command line.
Requirements for usage	You must have an uptodate LLVM system installed.
Creator	Matthias Klose, Sylvestre Ledru, Gianfranco Costamagna

Tool: NASM shell

Purpose	NASM is an assembler used to convert assembly to machine byte code.
command line or graphical?	Command line.
Requirements for usage	You must have NASM installed, and programs must be saved with the .asm file extension.
Creator	Simon Tatham

Exploitation Tools

Tool: searchsploit

Purpose	Used to search through the exploited database archive.
command line or graphical?	Command line.
Requirements for usage	Must have exploitdb package installed. Must have the title and path of the exploit.
Creator	Kali Linux

Tool: metasploit framework

Purpose	Metasploit is used to develop code to execute against target machines to find and exploit vulnerabilities.
command line or graphical?	Command line.
Requirements for usage	You must add a workspace upon entering the msf console. You must also have the IP of the target to exploit them.
Creator	Rapid7

Sniffing & Spoofing

Tool: ettercap-graphical

Purpose	The purpose of this application is to prompt ‘man in the middle’ type attacks.
command line or graphical?	Graphical.
Requirements for usage	Prior to usage you must have all dependencies installed. You must have at least two host targets.
Creator	Alberto Ornaghi (ALoR), Marco Valleri (NaGA), Emilio Escobar (exfil), Eric Milam (J0hnnyBrav0), Gianfranco Costamagna (LocutusOfBorg)

Tool: netsniff-ng

Purpose	The purpose of netsniff is to record pcap files to disc, as well as capture and replay packets.
command line or graphical?	Command line.
Requirements for usage	You must have a target website, and know if the packet configuration is high speed or not. You should also have a program to analyze the packet dump stored in a pcap file.
Creator	Daniel Borkmann, Tobias Klauser, Herbert Haas, Emmanuel Roullit, Markus Amend and many others

Post Exploitation

Tool: mimikatz

Purpose	Mimikatz is a post exploitation tool used to steal login credentials as well as escalate privileges. Specifically Mimikatz is used to print passwords to txt files.
command line or graphical?	Command line.
Requirements for usage	You must be compromising a windows machine that is 32 or 64 bit in architecture. You must also be using the Metasploit framework along with mimikatz.
Creator	Benjamin Delpy

Tool: weevely

Purpose	This program is used for post exploitation: a backdoor, or to manage web accounts. It acts like a telnet connection.
command line or graphical?	Command line.
Requirements for usage	You must have the PHP programming language on your computer. Inside the PHP file, you must contain the password to the backdoor.
Creator	Weevely Developers

Forensics

Tool: autopsy

Purpose	This program is used to recover data from a computer.
command line or graphical?	Begins in command line, and becomes graphical.
Requirements for usage	You must input case information such as : the case name, description and investigator names prior to using autopsy. You must have the host name of the computer you are investigating. You must also have access to the disk image.
Creator	Brian Carrier

Tool: hashdeep

Purpose	The purpose of hashdeep is to process, match, and audit hashsets. This can also be used to locate hash collisions, as well as report files not within the hashset.
command line or graphical?	Command line.
Requirements for usage	You must have the files to hash or analyze.
Creator	Jesse Kornblum

Reporting Tools

Tool: pipal

Purpose	This tool is used to analyse the statistics and information regarding user passwords.
command line or graphical?	Command line.
Requirements for usage	You must have a wordlist / file as input.
Creator	Robin Wood

Tool: faraday IDE

Purpose	The purpose faraday is to provide an IDE for critical analysis, distribution, as well as location of the data generated through the process of a security audit.
command line or graphical?	Command line and graphical.
Requirements for usage	You must have nmap installed and complete an nmap scan. Hopefully there will be a host you can scan and obtain vulnerabilities and host details.
Creator	Infobyte LLC

Social Engineering Tools

Tool: msf payload creator

Purpose	Used to create multiple types of payloads to target a system without an exploit.
command line or graphical?	Command line.
Requirements for usage	You must have the IP address and port number of the monitor interface you are attacking. You also need to know the type of machine you are attacking (Windows, Linux, ext.) You also need to know the information about the direction, stage, method, and CMD of the target/payload you want to create.
Creator	g0tmi1k

Tool: social engineering toolkit

Purpose	This is used for penetration testing, specifically regarding custom attacks through the use of social engineering.
command line or graphical?	Command line.
Requirements for usage	You must agree to the terms of usage prior to usage of the application. You must also know which social engineering type attack you would like to commit. In turn, you also need to know the associated knowledge required for each attack.
Creator	Dave Kennedy TrustedSec, LLC

System Services

Tool: Nessus

Purpose	This program is used to remotely scan a computer and notify the user about any possible vulnerabilities.
command line or graphical?	Graphical
Requirements for usage	You must register and obtain an access code to use this program. You must create a username and password. You must have endpoints or hosts to scan.
Creator	Renaud Deraison

All other system services have been previously completed within this document.