Tool Summary

27 February 2021 12:31

Tool Name	Purpose	Key Features	Imp. Links
ICE Swords	Anti-Rootkit	• It was coded by a Chinese programmer with a nickname as PJF. • Though it is more powerful than any other rootkit detection tools, it hasn't got much attention that other tools have received. • ICE Sword can find the rootkits which even top ant rootkit software (such as Rootkit Revealer, Blacklight, Rootkit Detective etc.) failed to detect. • However ICE Sword lack automatic file scanning, registry scanning feature that other anti-rootkits offer	• https://icesword.en.softonic.com/ • https://securityxploded.com/icesword.php
F-secure Blacklight	Anti-Rootkit	• detects objects that are hidden from users and security tools and offers the user an option to remove them • rootkits and all kinds of malware that use rootkits. • correctly ignore non-malicious objects and alerts only on real rootkits, which makes it useful even for users without technical knowledge. • This makes it possible to use it in the background without interrupting normal work.	• https://www.majorgeeks.com/files/details/f_secure_blacklight.html
Rootkit Revealer	Anti-Rootkit	• From Microsoft Sysinternals utility set • successfully detects many persistent rootkits including AFX, Vanquish and HackerDefender (note: RootkitRevealer is not intended to detect rootkits like Fu that don't attempt to hide their files or registry keys)	• https://docs.microsoft.com/en-us/sysinternals/downloads/rootkit-revealer
Dark Spy	Anti-Rootkit	<TBD>	
system virginity verifier	Anti-Rootkit	<TBD>	
RK Detector	Anti-Rootkit	<TBD>	
BetterCap	MITM Attacks Sniffing	MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more	

NMap

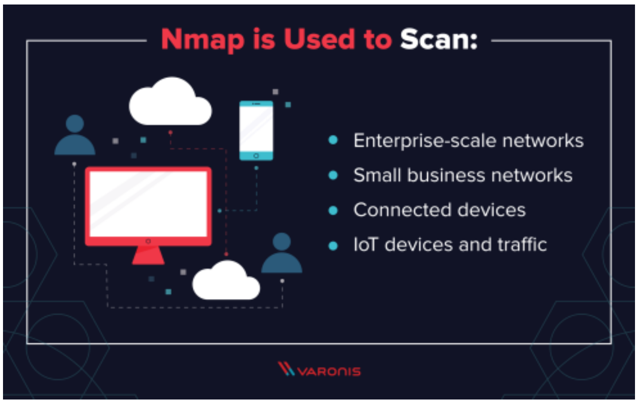
30 April 2021 21:56

- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.
- Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Nmap uses raw IP packets in novel ways to determine
    - what hosts are available on the network
    - what services (application name and version) those hosts are offering
    - what operating systems (and OS versions) they are running,
    - what type of packet filters/firewalls are in use, and dozens of other characteristics.
- It was designed to rapidly scan large networks, but works fine against single hosts.

Nmap is ...

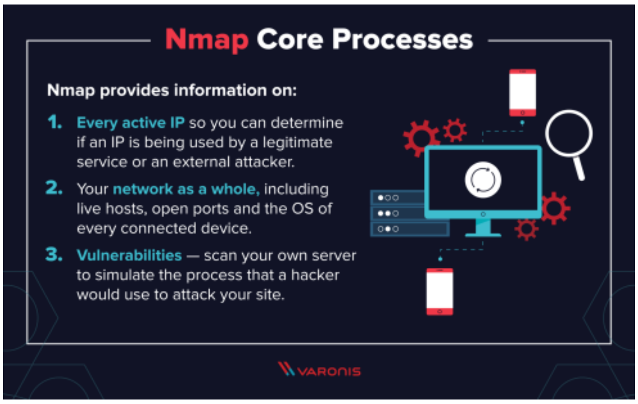
- **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- **Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- **Well Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- **Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.
- **Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.
- **Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

From <https://nmap.org/>



Nmap is Used to Scan:

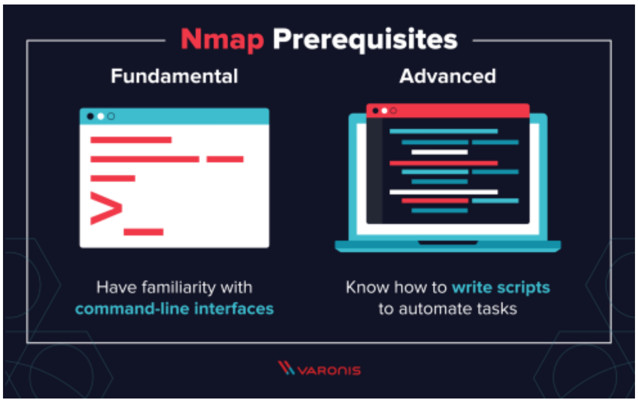
- Enterprise-scale networks
- Small business networks
- Connected devices
- IoT devices and traffic



Nmap Core Processes

Nmap provides information on:

1. Every active IP so you can determine if an IP is being used by a legitimate service or an external attacker.
2. Your network as a whole, including live hosts, open ports and the OS of every connected device.
3. Vulnerabilities — scan your own server to simulate the process that a hacker would use to attack your site.



Nmap Prerequisites

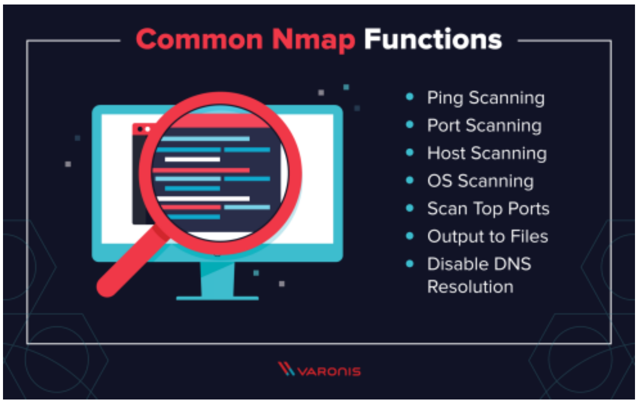
Fundamental

Have familiarity with **command-line interfaces**

Advanced

Know how to **write scripts** to automate tasks

VARONIS



Common Nmap Functions

- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution

VARONIS

Shodan

11 February 2021 19:42

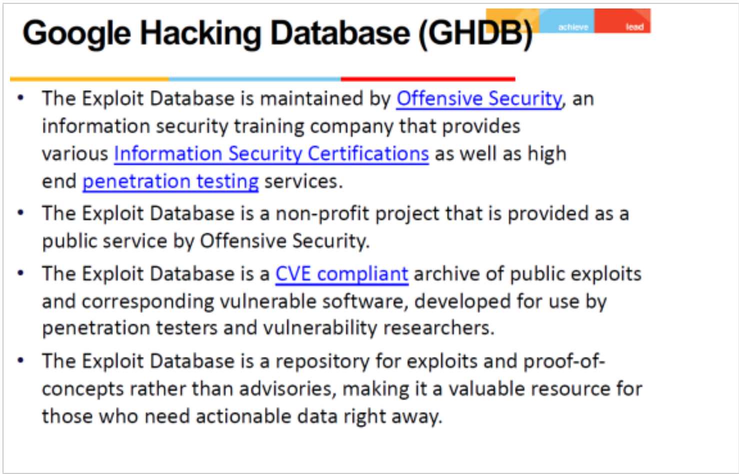
	Links
• Shodan is a search engine for internet connected device - Means if something is connected on internet - mostly it will be discoverable under Shodan • This is not always possible - BlackList • Competitive advantage - Who is using your competitors product, where, what kind of other software are running etc. • Usage for Pen testing and testing our own network • Similar to Google Dorking - Leveraging the Google search engine for reconnaissance phase • Shodan is just a web page • Shodan is a close source **How Shodan Works ?** • It uses '' Home grown, distributed port scanner" • Distributed port scanner ex : Nmap, Unicornscan, AngryIP Scan, NetCat, ZenMap, MASSCAN, RustScan • **Is it Illegal ?** • Masscan is dangerous compared to Shodan - masscan offers our network details to the target but shodan doesn't • Shodan is making connection to the network, comes back with result and aggregating the info for your behalf - our IP or network info is not getting shared to others • Shodan is probably safer than Masscan as you are moving the burden of performing the scanning from your control to someone else. • Widespread Scanning could fall into several provisions revolving around scanning. • "intentionally access a computer without authorization or exceed authorized access, and thereby obtain … information from any protected computer[.]" • "knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer[.]" • "intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage[.]" • "intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss[.]" • Accessing information via Shodan is safe as Shodan probably already having those data - we are simply using it **Why use Shodan?** • Easy to use compared to tools like Masscan • It can be a daunting task to install Elastic Search, deploy Masscan, parse the results, upload to their server, and then search and peer through the data • Shodan simplifies this mess by doing all of the heavy lifting for you	• https://retro64xyz.gitlab.io/presentations/2018/07/07/introduction-to-shodan/ https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/

GHDB

10 February 2021 20:11

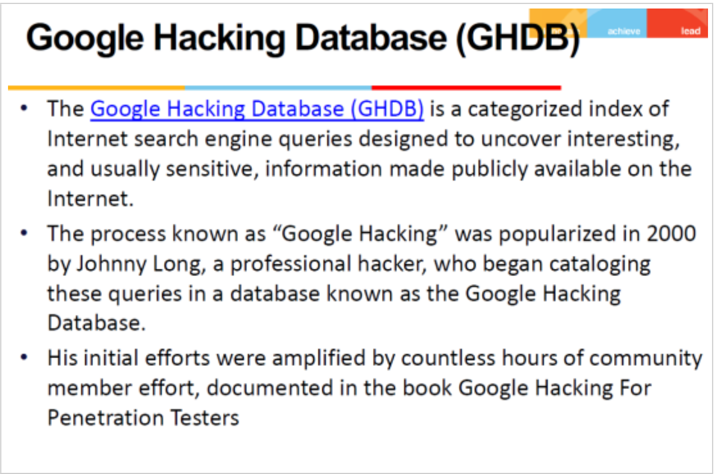
https://www.exploit-db.com/

https://www.exploit-db.com/papers



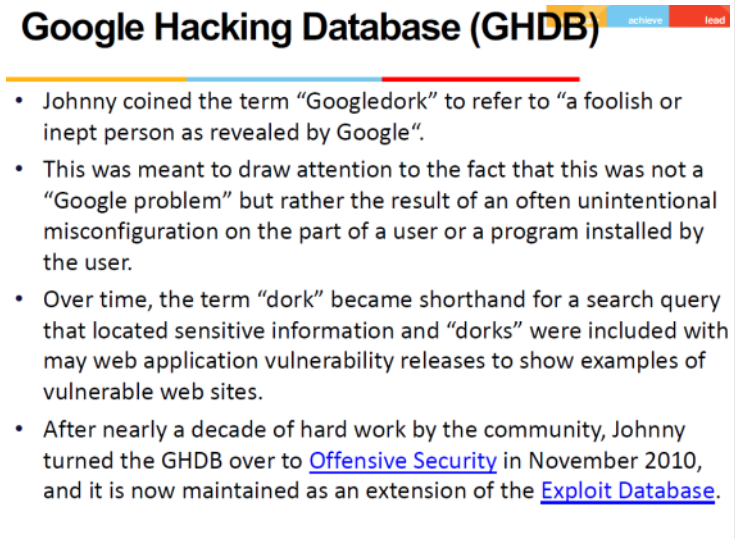
Google Hacking Database (GHDB)

- The Exploit Database is maintained by Offensive Security, an information security training company that provides various Information Security Certifications as well as high end penetration testing services.
- The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.
- The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.
- The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.



Google Hacking Database (GHDB)

- The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet.
- The process known as "Google Hacking" was popularized in 2000 by Johnny Long, a professional hacker, who began cataloging these queries in a database known as the Google Hacking Database.
- His initial efforts were amplified by countless hours of community member effort, documented in the book Google Hacking For Penetration Testers



Google Hacking Database (GHDB)

- Johnny coined the term "Googledork" to refer to "a foolish or inept person as revealed by Google".
- This was meant to draw attention to the fact that this was not a "Google problem" but rather the result of an often unintentional misconfiguration on the part of a user or a program installed by the user.
- Over time, the term "dork" became shorthand for a search query that located sensitive information and "dorks" were included with may web application vulnerability releases to show examples of vulnerable web sites.
- After nearly a decade of hard work by the community, Johnny turned the GHDB over to Offensive Security in November 2010, and it is now maintained as an extension of the Exploit Database.

Maltego

15 February 2021 22:30

Maltego is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks.

Transforms are small pieces of code that automatically fetch data from different sources and return the results as visual entities in the desktop client. Transforms are the central elements of Maltego which enable its users to unleash the full potential of the software whilst using a point-and-click logic to run analyses.

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.

What does Maltego do?
Maltego is a program that can be used to determine the relationships and real world links between:

- People
- Groups of people (social networks)
- Companies
- Organizations
- Web sites
- Internet infrastructure such as:
- Domains
- DNS names
- Netblocks
- IP addresses
- Phrases
- Affiliations
- Documents and files
- These entities are linked using open source intelligence.
- Maltego is easy and quick to install – it uses Java, so it runs on Windows, Mac and Linux.
- Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate – making it possible to see hidden connections.
- Using the graphical user interface (GUI) you can see relationships easily – even if they are three or four degrees of separation away.
- Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

From <https://tools.kali.org/information-gathering/maltego-teeth>

What can Maltego do for me?

- Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter.
- Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items.
- Maltego provide you with a much more powerful search, giving you smarter results.
- If access to "hidden" information determines your success, Maltego can help you discover it.

Source: http://paterva.com/web6/products/maltego.php
Maltego Homepage | Kali Maltego Teeth Repo

- Author: Paterva
- License: Commercial

From <https://tools.kali.org/information-gathering/maltego-teeth>

GNS3 - Graphical Network Simulator-3

22 February 2021 13:20

GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

GNS3 is open source, free software that you can download from http://gns3.com

It is actively developed and supported and has a growing community of over 800,000 members. By joining the GNS3 community you will be joining fellow students, network engineers, architects and others that have downloaded GNS3 over 10 million times to date. GNS3 is used in companies all over the world including Fortune 500 companies.

GNS3 can help you prepare for certification exams such as the Cisco CCNA, but also help you test and verify real world deployments. Jeremy Grossman, the original developer of GNS3 originally created the software to help him study for his CCNP certifications. Because of that original work, you can today use to help you do the same without paying for expensive hardware.

GNS3 has allowed network engineers to virtualize real hardware devices for over 10 years. Originally only emulating Cisco devices using software called Dynamips, GNS3 has now evolved and supports many devices from multiple network vendors including Cisco virtual switches, Cisco ASAs, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, multiple Linux appliances and many others. Go here to see a list of appliances available: https://gns3.com/marketplace/appliances

Kali Linux

10 February 2021 16:16

Crunch
RainbowCrack

Ghidra

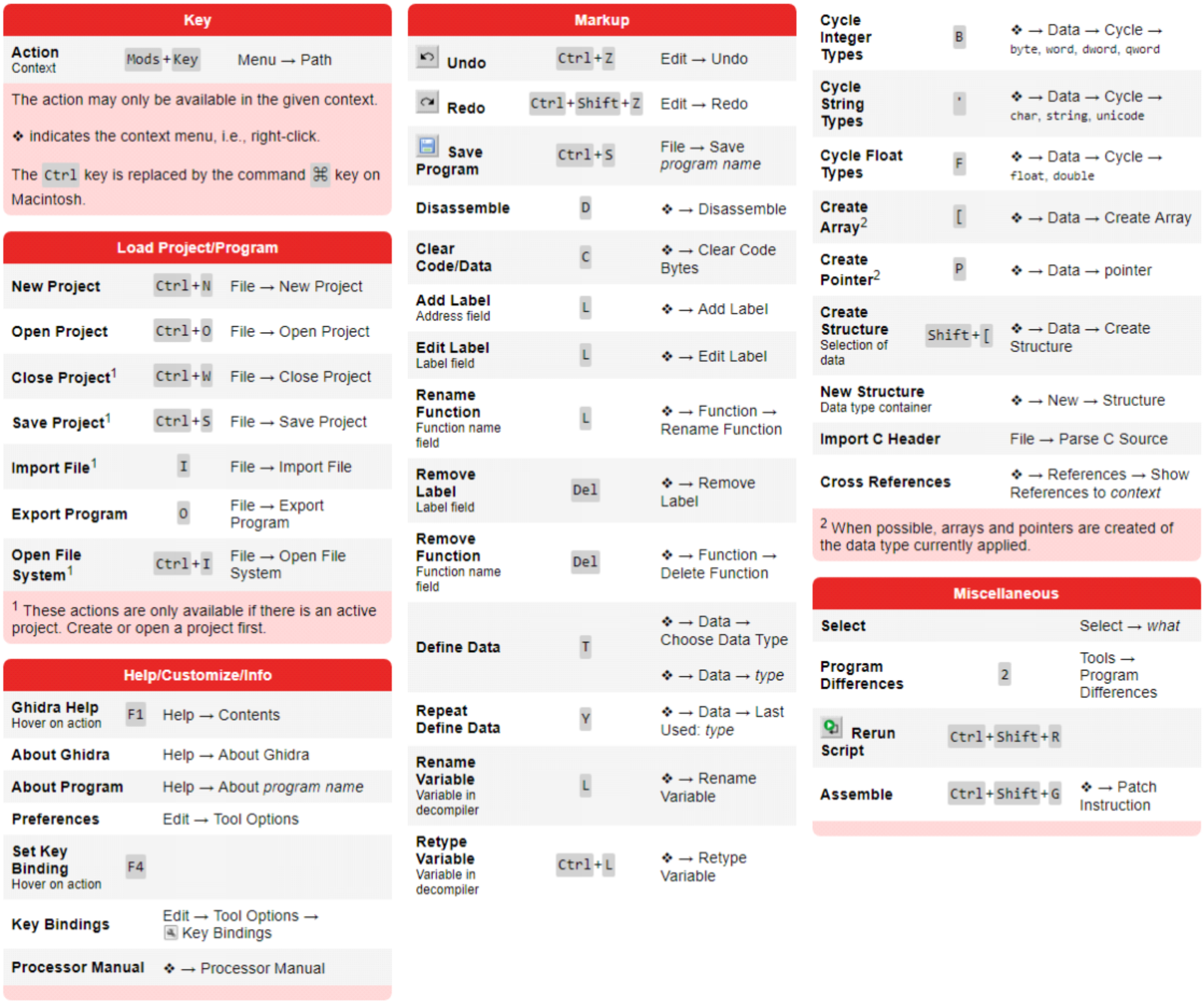
11 February 2021 08:44

https://ghidra-sre.org/

IDA-Pro Hex Rays (current ver 7.5) - https://www.hex-rays.com
- CFE Explorer
- API Monitor
- WinHex
- Hiew
- Fiddler
- Scylla
- Relocation Section Editor
- PEiD

Key features :

- includes a suite of software analysis tools for analyzing compiled code on a variety of platforms including Windows, Mac OS, and Linux
- capabilities include disassembly, assembly, decompilation, graphing and scripting, and hundreds of other features
- supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes.
- users may develop their own Ghidra plug-in components and/or scripts using the exposed API



Key

Action Context	Mods+Key	Menu → Path

The action may only be available in the given context.

❖ indicates the context menu, i.e., right-click.

The Ctrl key is replaced by the command ⌘ key on Macintosh.

Load Project/Program

New Project	Ctrl+N	File → New Project
Open Project	Ctrl+O	File → Open Project
Close Project[1]	Ctrl+W	File → Close Project
Save Project[1]	Ctrl+S	File → Save Project
Import File[1]	I	File → Import File
Export Program	O	File → Export Program
Open File System[1]	Ctrl+I	File → Open File System

[1] These actions are only available if there is an active project. Create or open a project first.

Help/Customize/Info

Ghidra Help Hover on action	F1	Help → Contents
About Ghidra		Help → About Ghidra
About Program		Help → About *program name*
Preferences		Edit → Tool Options
Set Key Binding Hover on action	F4	
Key Bindings		Edit → Tool Options → Key Bindings
Processor Manual		❖ → Processor Manual

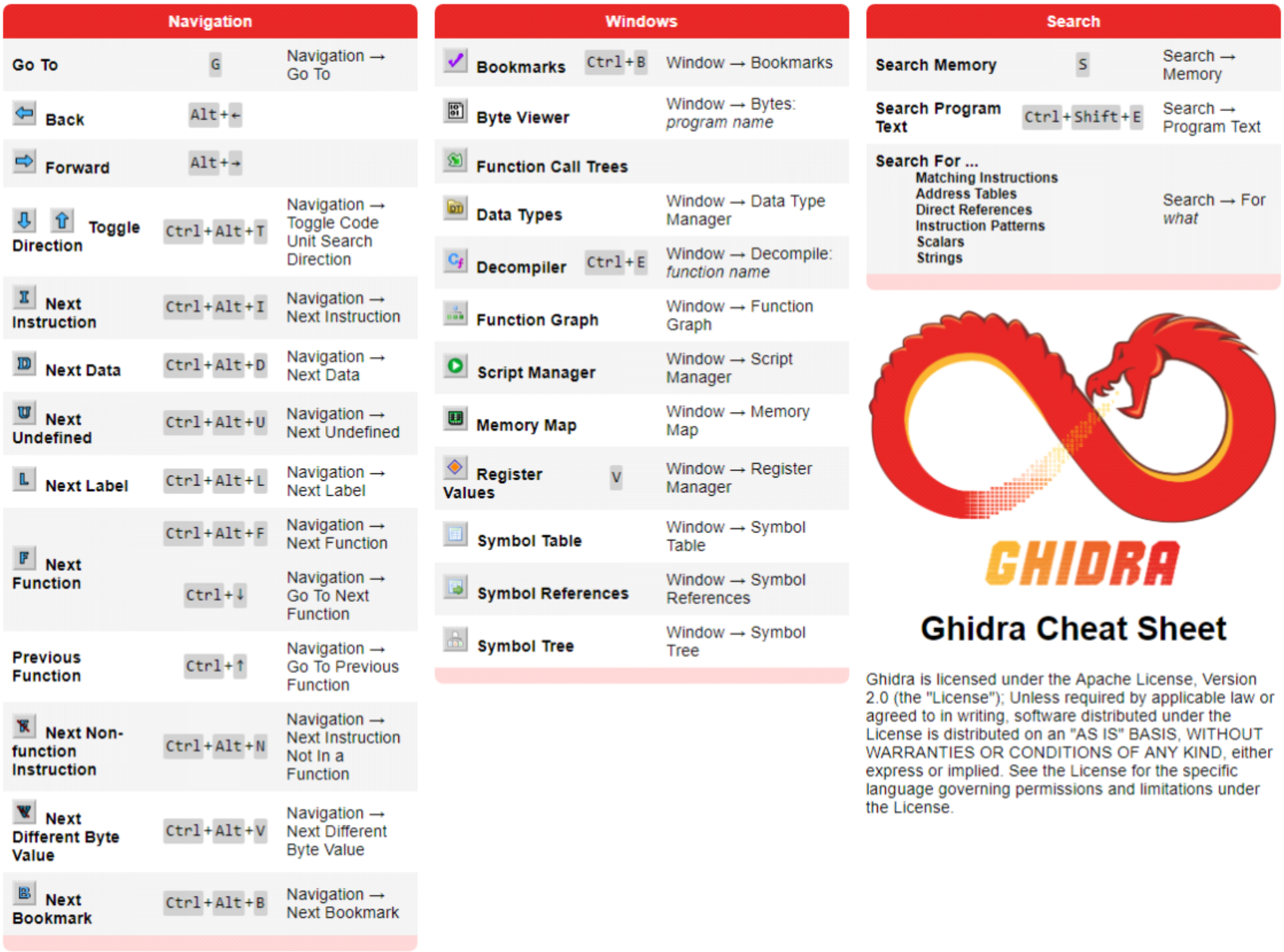
Markup

Undo	Ctrl+Z	Edit → Undo
Redo	Ctrl+Shift+Z	Edit → Redo
Save Program	Ctrl+S	File → Save *program name*
Disassemble	D	❖ → Disassemble
Clear Code/Data	C	❖ → Clear Code Bytes
Add Label Address field	L	❖ → Add Label
Edit Label Label field	L	❖ → Edit Label
Rename Function Function name field	L	❖ → Function → Rename Function
Remove Label Label field	Del	❖ → Remove Label
Remove Function Function name field	Del	❖ → Function → Delete Function
Define Data	T	❖ → Data → Choose Data Type ❖ → Data → *type*
Repeat Define Data	Y	❖ → Data → Last Used: *type*
Rename Variable Variable in decompiler	L	❖ → Rename Variable
Retype Variable Variable in decompiler	Ctrl+L	❖ → Retype Variable
Cycle Integer Types	B	❖ → Data → Cycle → byte, word, dword, qword
Cycle String Types	'	❖ → Data → Cycle → char, string, unicode
Cycle Float Types	F	❖ → Data → Cycle → float, double
Create Array[2]	[	❖ → Data → Create Array
Create Pointer[2]	P	❖ → Data → pointer
Create Structure Selection of data	Shift+[	❖ → Data → Create Structure
New Structure Data type container		❖ → New → Structure
Import C Header		File → Parse C Source
Cross References		❖ → References → Show References to *context*

[2] When possible, arrays and pointers are created of the data type currently applied.

Miscellaneous

Select		Select → *what*
Program Differences	2	Tools → Program Differences
Rerun Script	Ctrl+Shift+R	
Assemble	Ctrl+Shift+G	❖ → Patch Instruction



Navigation		
Go To	G	Navigation → Go To
Back	Alt+←	
Forward	Alt+→	
Toggle Direction	Ctrl+Alt+T	Navigation → Toggle Code Unit Search Direction
Next Instruction	Ctrl+Alt+I	Navigation → Next Instruction
Next Data	Ctrl+Alt+D	Navigation → Next Data
Next Undefined	Ctrl+Alt+U	Navigation → Next Undefined
Next Label	Ctrl+Alt+L	Navigation → Next Label
Next Function	Ctrl+Alt+F	Navigation → Next Function
	Ctrl+↓	Navigation → Go To Next Function
Previous Function	Ctrl+↑	Navigation → Go To Previous Function
Next Non-function Instruction	Ctrl+Alt+N	Navigation → Next Instruction Not In a Function
Next Different Byte Value	Ctrl+Alt+V	Navigation → Next Different Byte Value
Next Bookmark	Ctrl+Alt+B	Navigation → Next Bookmark

Windows		
Bookmarks	Ctrl+B	Window → Bookmarks
Byte Viewer		Window → Bytes: *program name*
Function Call Trees		
Data Types		Window → Data Type Manager
Decompiler	Ctrl+E	Window → Decompile: *function name*
Function Graph		Window → Function Graph
Script Manager		Window → Script Manager
Memory Map		Window → Memory Map
Register Values	V	Window → Register Manager
Symbol Table		Window → Symbol Table
Symbol References		Window → Symbol References
Symbol Tree		Window → Symbol Tree

Search		
Search Memory	S	Search → Memory
Search Program Text	Ctrl+Shift+E	Search → Program Text
Search For ... Matching Instructions Address Tables Direct References Instruction Patterns Scalars Strings		Search → For *what*

GHIDRA

Ghidra Cheat Sheet

Linux vs Unix

11 February 2021 09:01

Following are the important difference between Linux and Unix.

Sr. No.	Key	Linux Linux is a clone of Unix	Unix
1	Development	Linux is open source and is developed by Linux community of developers. Linux is Open Source, and thousands of programmer collaborate online and contribute to its development. The source is available to the general public	Unix was developed by AT&T Bell labs and is not open source. Unix systems have different versions. These versions are primarily developed by AT&T as well as other commercial vendors. The source code is not available to anyone.
2	Cost	Linux is free to use. Linux is freely distributed, downloaded through magazines, Books, website, etc. There are paid versions also available for Linux.	Unix is licensed OS. Different flavors of Unix have different pricing depending upon the type of vendor.
3	Supported File systems	Ext2, Ext3, Ext4, Jfs, ReiserFS, Xfs, Btrfs, FAT, FAT32, NTFS.	fs, gpfs, hfs, hfs+, ufs, xfs, zfs.
4	GUI	Linux uses KDE and Gnome. Other GUI supported are LXDE, Xfce, Unity, Mate.	Unix was initially a command based OS. Most of the unix distributions now have Gnome.
5	Usage	Linux is used in wide varieties from desktop, servers, smartphones to mainframes. Everyone. From home users to developers and computer enthusiasts alike.	Unix is mostly used on servers, workstations or PCs. The UNIX can be used in internet servers, workstations, and PCs.
6	Default Shell	Bash (Bourne Again SHell) is default shell for Linux.	Bourne Shell is default shell for Unix.
7	Architecture	Linux was initially developed for Intel's x86 hardware processors. Now it supports 20+ processor families. Initially developed for Intel's x86 hardware processors. It is available for over twenty different types of CPU which also includes an ARM.	CUnix supports PA-RISC and Itanium family.
9	Virus	Linux has had about 60-100 viruses listed to date which are currently not spreading.	There are between 80 to 120 viruses reported till date in Unix.
10	Thread detection	Threat detection and solution is very fast because Linux is mainly community driven. So, if any Linux user posts any kind of threat, a team of qualified developers starts working to resolve this threat.	Unix users require longer wait time, to get the proper bug fixing patch.
11	Best feature	Kernel update without reboot	Feta ZFS - next generation filesystem DTrace - dynamic Kernel Tracing
12	Portability	Linux is portable and is booted from a USB Stick	Unix is not portable
13	Features	• Support multitasking • Programs consist of one or more processes, and each process have one or more threads • It can easily co-exists along with other Operating systems. • Linux can run multiple user programs • Individual accounts are protected because of appropriate authorization • Linux is a replica of UNIX but does not use its code.	• Unix is a Multi-user, multitasking operating system • It can be used as the master control program in workstations and servers. • Hundreds of commercial applications are available • In its heydays, UNIX was rapidly adopted and became the standard OS in university
14	Limitations	• For Linux vs Unix, There's no standard edition of Linux • Linux has patchier support for drivers which may result in misfunctioning of the entire system. • Linux is, for new users at least, not as easy to use as Windows. • Many of the programs we are using for Windows will only run on Linux only with the help of a complicated emulator. For example. Microsoft Office. • Linux is best suitable for a corporate user. It's much harder to introduce in a home setting.	• The unfriendly, terse, inconsistent, and non-mnemonic user interface • Comparing limitation of Linux vs Unix, Unix OS is designed for a slow computer system, so you can't expect fast performance. • Shell interface can be treacherous because typing mistake can destroy files. • Versions on various machines are slightly different, so it lacks consistency. • Unix does not provide any assured hardware interrupt response time, so it does not support real time response time systems.
15	Example	Redhat, OpenSuse,Ubuntu, Debian GNU, Arch Linux, etc.	SunOS, Solaris, SCO UNIX, AIX, HP/UX, ULTRIX etc.

From <https://www.tutorialspoint.com/difference-between-linux-and-unix>

Google Dorks

12 January 2021 17:43

Imp Links:

- https://exposingtheinvisible.org/guides/google-dorking/
- https://whatis.techtarget.com/definition/Google-dork-query
- https://www.exploit-db.com/google-hacking-database
- https://www.exploit-db.com/?platform=android
- https://gist.github.com/stevenswafford/393c6ec7b5375d5e8cdc

Tool :

- https://github.com/sundowndev/dorkgen

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website.

Google Dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. That description includes information that is not intended for public viewing but that has not been adequately protected.

If you are thinking about using googleDorking as an investigative technique, there are several precautions to take. Although you are free to search at-will on search engines, accessing certain webpages or downloading files from them can be a prosecutable offense, especially in the United States in accordance with the extremely vague and overreaching Computer Fraud and Abuse Act (CFAA). Moreover, if you're dorking in a country with heavy internet surveillance (i.e. any country), it's possible that your searches could be recorded and used against you in the future.

Use TOR browser

Example:

- hacking exposed 7 **filetype:**pdf
- **site:**mastercard.com **filetype:**pdf
- **inurl:** free assassin's creed valhalla
- intext:mobile number filetype:xls
  - https://www.rsb.edu.in/RSB_Student_details_2019_2020.xls (Rajlakshmi School of Business)
- filetype: doc filetype:pdf "Aadhar" site:gov.in

E7705800

lifeline

```
export GOPATH=/root/go-workspace
export GOROOT=/home/kali/Desktop/Tools/PhoneInfoGa/go/
PATH=$PATH:$GOROOT/bin/:$GOPATH/bin
```

Aircrack

27 February 2021 11:42

- Aircrack can be used for 802.11a/b/g WEP and WPA cracking.
- Aircrack uses algorithms to recover wireless passwords by capturing packets. Once enough packets have been gathered, it tries to recover the password.
- To make the attack faster, it implements a standard FMS attack with some optimizations.
- It supports most of the wireless adapters
- It requires deeper knowledge of Linux. If you are not comfortable with Linux, you will find it hard to use this tool.
- Ref: http://www.aircrack-ng.org

- Aircrack-ng is a tool that comes pre-installed in Kali Linux and is used for wifi network security and hacking.
- Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool.
- It is a tool used for wifi hacking.
- It helps in capturing the package and reading the hashes out of them and even cracking those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces.
- It mainly focuses on 4 areas:
  - Monitoring: Captures cap, packet, or hash files.
  - Attacking: Performs deauthentication or creates fake access points
  - Testing: Checking the wifi cards or driver capabilities
  - Cracking: Various security standards like WEP or WPA PSK.

<< See PDF >>

Net Stumbler

27 February 2021 11:45

- Shareware tool written for Windows that enables to detect WLANs
  - Supports 802.11a, 802.11b, and 802.11g standards
- NetStumbler was primarily designed to

  – Verify WLAN configuration
  – Detect other wireless networks
  – Detect unauthorized Aps
  – Wardriving
- NetStumbler is capable of interface with a GPS
  - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

- NetStumbler logs the following information

  – SSID
  – MAC address of the AP
  – Manufacturer of the AP
  – Channel on which it was heard
  – Strength of the signal
  – Encryption
- Attackers can detect APs within a 350-foot radius with a good antenna, they can locate APs a couple of miles away

The importance of wireless is not a hidden truth, the technology world is going to be the wireless at the consumer side especially. So in this article we will talk about the wireless local area network (WLAN) detector tool.

NetStumbler formally known as Network Stumbler its probably the first wireless detection tool that people came across.

Netstumbler is design for the windows plate form, it works on windows based operating system.It can detect WiFi that is IEEE 802.11b, 802.11g and 802.11a networks. MiniStumbler is also available and works on Windows CE based system.

Commonly Used For

- Finding network configuration of AP (Access Point).
- Finding the cause of interference
- Finding the strength of the received signal
- Finding unauthorised access point.

Kismet

27 February 2021 11:47

- Another product for conducting wardriving attacks
    - Written by Mike Kershaw
- Runs on Linux, BSD, MAC OSX, and Linux PDAs
- Kismet can also act a sniffer and IDS
    - Kismet can sniff 802.11b, 802.11a, and 802.11g traffic
- Can detect wireless networks both visible and hidden, sniffer packets and detect intrusions

• For details refer: https://www.kismetwireless.net/

Kismet is an 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11a/b/g/n traffic. It can use other programs to play audio alarms for network events, read out network summaries, or provide GPS coordinates. This is the main package containing the core, client, and server.

Features

- Ethereal and Tcpdump compatible data logging
- AirSnort compatible
- Network IP range detection
- Hidden network SSID detection
- Graphical mapping of networks
- Client-server architecture
- Manufacturer and model identification of APs and clients
- Detection of known default access point configurations
- XML output
- Supports 20 card types

AirSnort

27 February 2021 11:49

- Created by Jeremy Bruestle and Blake Hegerle
- Can help access WEP-enabled WLAN
- Limitations
  – Runs only on Linux
  – Requires specific drivers
  – Not all wireless NICs function with AirSnort

AirSnort is a famous wireless LAN password cracking tool. You can hack WEP keys of the Wi-Fi802.11b network.This tool work on by observing devices. After collecting adequate packets, it works by computing the encryption key. This tool is free for Linux and Windows users. It is very easy to access. In spite not getting updated since last three years, it works very nicely. The company has decided to update it. It is linked straight to WEP hacking and therefore liked by most of the users.

WEPCrack

27 February 2021 11:49

- Open-source tool used to crack WEP encryption
- WEPCrack uses Perl scripts to carry out attacks on wireless systems
- Has features to conduct brute-force attack
- For details refer: http://wepcrack.sourceforge.net/

- WebDecrypt: this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. http://wepdecrypt.sourceforge.net/

OSINT

09 March 2021 09:45

What ?	• Open-Source Intelligence (OSINT) is a term that refers to all publicly available information that is used to meet a specific intelligence need • refers to the collection and analysis of publicly available information, mostly from online sources. • OSINT resources can take two forms, offline or online. However, with the ongoing digitalization of the world, most of the OSINT intelligence is now taken from Internet resources. • The huge amount of digital data is considered the biggest challenge of any OSINT collection activity. • there is a plethora of OSINT tools and techniques that can be used to assist the OSINT assemblies in this task
Links	• https://traversals.com/blog/osint/ • https://traversals.com/blog/osint-tools/#:~:text=Open%2Dsource%20intelligence%20(OSINT),of%20any%20OSINT%20collection%20activity.
Why Imp ?	• Discovering public-facing assets : • Their most common function is helping IT teams discover public facing assets and mapping what information each possesses thatcould contribute to a potential attack surface • Discover relevant information outside the organization : • A secondary function that some OSINT tools perform is looking for relevant information outside of an organization, such as insocial media posts or at domains and locations that might be outside of a tightly defined network • Collate discovered information into actionable form : • some OSINT tools help to collate and group all the discovered information into useful and actionable intelligence.
Tools	• Maltego • Recon-ng • theHarvester • Shodan • Metagoofil • Searchcode • SpiderFoot • Babel X • https://inteltechniques.com/ • https://null-byte.wonderhowto.com/how-to/hunt-down-social-media-accounts-by-usernames-with-sherlock-0196138/
E.g.	• https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/ • https://github.com/sundowndev/PhoneInfoga • https://sundowndev.github.io/PhoneInfoga/ • Windows Command : ○ cd "E:\MTech\SEM 2\Ethical Hacking SS ZG575 - 3\Tools\PhoneInfoga_Windows_x86_64" ○ phoneinfoga scan -n +919904705162 ○ phoneinfoga help • https://inteltechniques.com/ • Sherlock • https://github.com/sherlock-project/sherlock • python3 sherlock.py namegoeshere --print-found • Beacon Swarm - https://archive.org/details/youtube-o95Or-Z_Ybk • Smartphones and laptops are constantly sending Wi-Fi radio signals, and many of these signals can be used to track us • we'll program a cheap IoT device in Arduino to create hundreds of fake networks with common names; • This will cause nearby devices to reveal their real trackable MAC address, and it can even let an attacker take over the phone's data connection with no warning
OSINT Framework	https://osintframework.com/

Cain and Able

01 May 2021 06:10

<< See PDF >>

https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/

SMAP

01 May 2021 06:21

<< See PDF under Materials>>

SIPVicious

01 May 2021 06:23

SIPVicious suite is a set of tools that can be used to audit SIP based VoIP systems

It currently consists of four tools:.

- svmap – this is a sip scanner. Lists SIP devices found on an IP range
- svwar – identifies active extensions on a PBX
- svcrack – an online password cracker for SIP PBX
- svreport – manages sessions and exports reports to various formats
- svcrash – attempts to stop unauthorized svwar and svcrack scans.

Nikto

01 May 2021 06:34

- Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items,
    - including over 6700 potentially dangerous files/programs,
    - checks for outdated versions of over 1250 servers,
    - and version specific problems on over 270 servers
- It also checks for server configuration items such as
    - the presence of multiple index files,
    - HTTP server options, and will attempt to identify installed web servers and software.
    - Scan items and plugins are frequently updated and can be automatically updated.
- Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

<< See PDF under materials >>

Nessus

01 May 2021 06:36

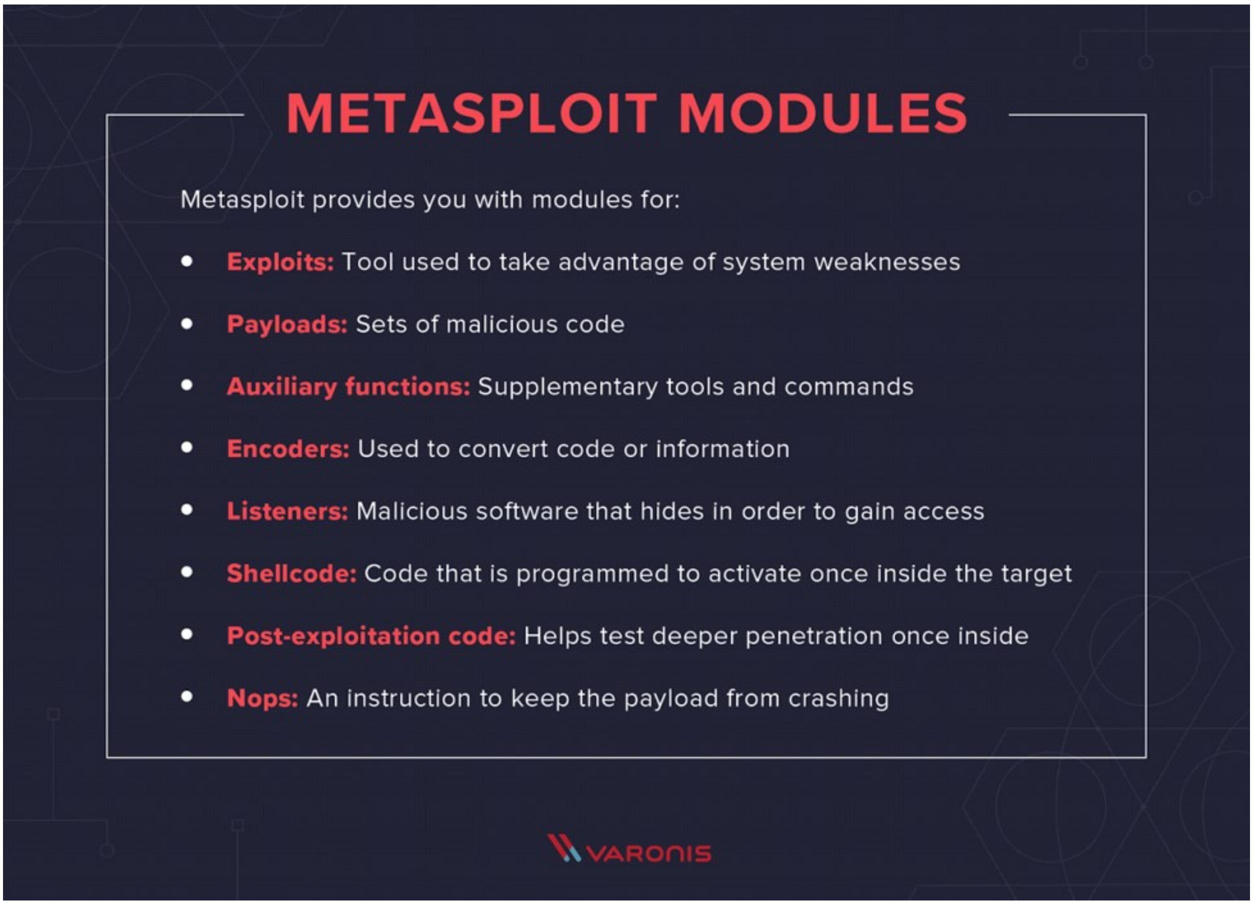
Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

<< See PDF under Materials >>

Metaspolit

01 May 2021 06:46

-
- << See PDF in Materials >>
- The Metasploit Framework is an open source penetration testing and development platform that provides exploits for a variety of applications, operating systems and platforms
- It provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing and thanks to the open source community and Rapid7's own hard working content team, new modules are added on a regular basis, which means that the latest exploit is available to you as soon as it's published.
- Metasploit is one of the most commonly used penetration testing tools and comes built-in to Kali Linux.
- The main components of the Metasploit Framework are called modules.
  - Modules are standalone pieces of code or software that provide functionality to Metasploit.
  - There are six total modules:
    - Exploits
    - Payloads
    - Auxiliary
    - Nops
    - Posts
    - Encoders
- Advantages :
  - Open source
  - Support for testing large networks and easy naming conventions
  - Smart payload generation and switching mechanism
  - Cleaner exits
  - The GUI environment

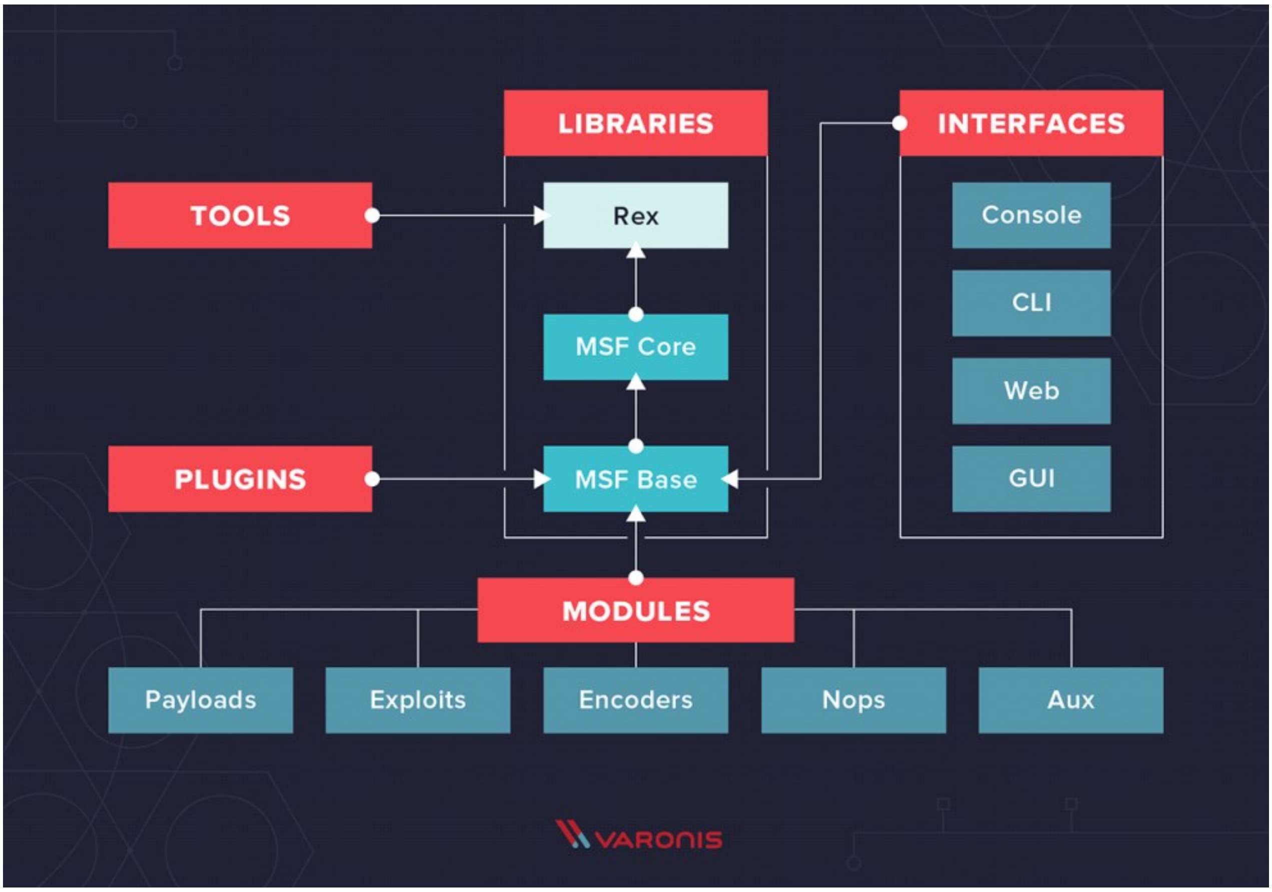


METASPLOIT MODULES

Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

VARONIS


LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux
VARONIS