REMA

Date: 05/02/25 Page No.

Topic:

(1) IDA Pro (Interactive DisAssemble):-

→ How it works:-

→ IDA pro is a disassembler and debugger that converts machine code into assembly, allowing in-depth analysis of binaries.

→ Installation:-

(1) Download from Hex-Rays website.
(2) Install using the provided installer and follow on-screen instructions.

→ CLI Commands :-

→ ida -B -S<script> <binary> :-
→ Open a binary in IDA pro with a script exe

→ ida64 -A <binary> :-
→ Run automatic analysis of the binary.

Topic:

(2) Ghidra :-

→ Ghidra is an open-source Reverse Engineering framework developed by the NSA for disassembly, decompilation and program analysis.

→ (1) Download from Ghidra website
(2) Extract the archive and Execute the application

→ Commands :-

→ analyzeHeadless <project-dir> <binary> - Import <binary> start headless analysis.
→ ghidraRun :- to launch Ghidra GUI.

3) ollyDbg :-

→ ollyDbg is a 32-bit debugger for analyzing windows binaries. It operates in Real-time to inspect memory, registers, and CPU instructions.

→ (1) Download from ollyDbg website.
(2) Extract and Run the executable.

→ Commands:-

→ OllyDbg is GUI-based and does not have extensive CLI support. Use scripts within the interface.

(4) Radare2:-

→ Radare2 is an open-source framework for reverse engineering. It supports disassembling, debugging, and decompiling various binary formats.

→ on Linux:- sudo apt install Radare2

→ on Windows:- Use the radare2 Github

→ Commands:-

→ r2 <binary> :- open a binary for analysis.
→ aa :- Analyze all functions.
→ pdf @ <address> :- Print disassembly at a specific address
→ db <address> :- Set a breakpoint at the given address.

Date: Page No.

Topic:

(5) x64dbg:-

→ x64dbg is an opensource debugger for windows applications, supporting both 32 bit and 64-bit binaries for dynamic analysis.

→ Download from x64dbg website.
→ Extract and run the executable

→ Commands:-

→ x64dbg <binary>:- open the binary file for analysis.
→ bp <address>:- Set a breakpoint at a given addr.

(6) Binwalk:-

→ Binwalk is used for analyzing and extracting firmware images. It can detect embedded files and compressed data in binary firmware.

→ On linux:- sudo apt install binwalk.

→ On windows:- Use WSL or a VM for Installation.

Topic: _____

→ Commands:-

→ binwalk <firmware-image>:- Analyze the firmware image.

→ binwalk -e <firmware-image>:- Extract embedded files from the firmware.

(7) Wireshark:-

→ Wireshark is a Network protocol analyzer that captures and analyzes network traffic. Useful for Software-Engineering network protocols.

→ Download from Wireshark website.

→ Install using the provided installer.

→ Commands:-

→ tshark -i <interface>:- Start capturing on the given Network interface.

→ tshark -r <file>:- Read from a capture file and analyze it.

Date: Page No.

Topic:

(8) Frida :-

→ Frida is a dynamic instrumentation toolkit for reverse-engineering mobile apps and analyzing running processes in real time.

→ Pip install frida tools.

→ Command :-

→ frida -U -f <add> -l <script.js> :- Inject a script into a mobile application.

→ frida -U -p <pid> -l <script.js> :- Attach to a running process and inject a script.

(9) Immunity Debuggers :-

→ Immunity Debugger is used for analyzing and debugging executables, often used in security research and exploit development.

→ Download from immunity website.

→ Run the installer.

Topic:

→ Immunity Debugger is GUI based, but can be controlled via python scripting for automation.

(10) PEiD :-

→ PEiD detects packers, cryptors, and protectors used to obfuscate executables. It identifies known packing methods.

→ Download from PEiD website.

→ Extract and run the executable.

→ Commands :-

→ GUI-based, so no major CLI supported exists.

(11) Apk Tools :-

→ Apk Tools used for decompiling and modifying Android apk files. it extracts resources and disassembles the code to ~~Smali~~ Smali.

Topic: _____

→ On Linux:- sudo apt install apktool.

→ On MacOSX:- brew install apktool

→ Commands:-

→ apk tool d <apk-file>
→ apk tool b <directory>.

(12) Burpsuite:-

→ Burp suite is used for security testing of web applications by intercepting, analyzing and manipulating HTTP/s traffic.

→ Download from Burpsuite website.
→ install and run the application.

→ Commands:-

→ Burpsuite is mostly GUI-based, but you can see the burpsuite command to launch it from the terminal.

(13) JEB Decompiler:-

→ JEB is a powerful decompiler for Android and other binaries that converts machine code into high-level languages for analysis.

→ Download from JEB website.
→ Install and launch.

→ GUI-Based, But automation can be done via the Java API.

(14) Decompile X :-

→ DecompileX is a decompiler for Android Apk files, transforming Apk bytecode into Java source code.

→ Download from GitHub Repository.
→ Extract and run the tool.

→ Commands

→ Java -jar DecompileX.jar <apk-file> :-
Decompile the Apk file.

Date: Page No.

Topic:

(25) VMP Emulator:-

→ VMP Emulator is used to Emulate virtual Machines based to Emulate protections in software, often used for Cracking or Unpacking.

→ Download from a trusted site. (use caution)

→ GUI Based but can be Controlled via External Scripts.

(26) PBViewer:-

→ Is used for inspecting the internals of PE (Portable Executable) files, including headers, Sections and Resources.

→ Download from PBViewer website.
→ Extract and Run the Executable.

→ Gui based.

Date: _____ Page No.

Topic: _____

(17) Sysinternals Suite:-

→ This include a collection of Windows system tools for monitoring, troubleshooting, and analyzing processes.

→ Download from sysinternals website.
→ Extract and Run the tools.

→ Commands:-

→ Pslist
→ Procmon
→ autoruns.

(18) Cutter :-

→ Cutter is a GUI frontend for Radare2, simplifying reverse engineering tasks with an intuitive interface.

→ Download from Cutter website.
→ Install and launch.

Date: _____ Page No.

Topic: _____

→ 32 things for analysis

(19) Hopper Disassembler

→ Hopper is a macos and Linux that allows the analysis of executable by converting machine code into assembly or high level code.

→ Download from Hopper website
→ Install and launch

→ Commands

→ Limited CLI Support.

(20) Telerik Just Decompiler

→ This is a .Net decompiler used for source engineering .Net assemblies and converting them into Readable Source Code.

→ Download from Telerik Website.
→ install and Run the application

→ Just decompile assemblys :- Decompile a .Net assembly file.