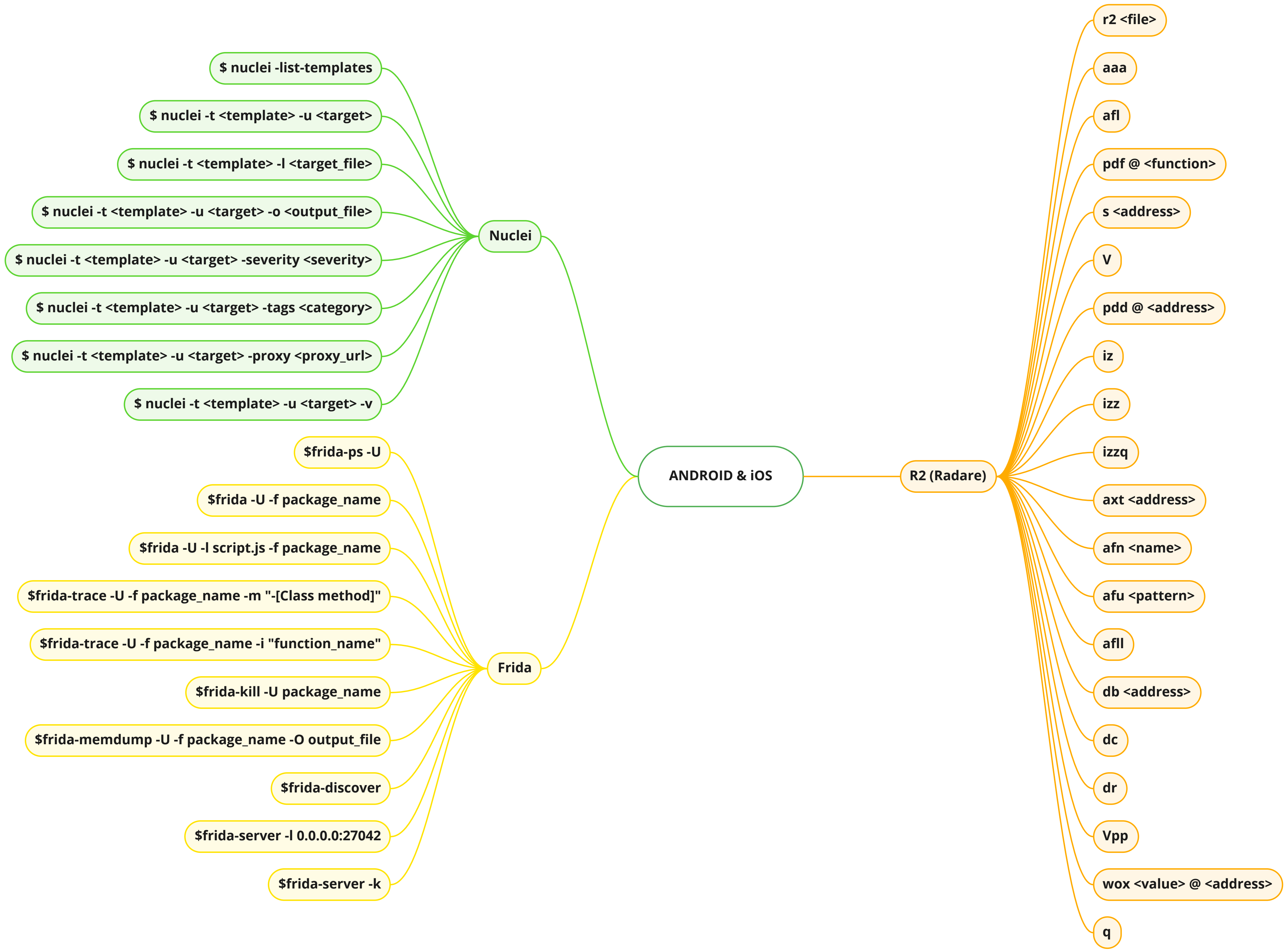
Android & iOS Cheatsheet MindMap



- ANDROID & iOS
  - Nuclei
    - $ nuclei -list-templates
    - $ nuclei -t <template> -u <target>
    - $ nuclei -t <template> -l <target_file>
    - $ nuclei -t <template> -u <target> -o <output_file>
    - $ nuclei -t <template> -u <target> -severity <severity>
    - $ nuclei -t <template> -u <target> -tags <category>
    - $ nuclei -t <template> -u <target> -proxy <proxy_url>
    - $ nuclei -t <template> -u <target> -v
  - Frida
    - $frida-ps -U
    - $frida -U -f package_name
    - $frida -U -l script.js -f package_name
    - $frida-trace -U -f package_name -m "-[Class method]"
    - $frida-trace -U -f package_name -i "function_name"
    - $frida-kill -U package_name
    - $frida-memdump -U -f package_name -O output_file
    - $frida-discover
    - $frida-server -l 0.0.0.0:27042
    - $frida-server -k
  - R2 (Radare)
    - r2 <file>
    - aaa
    - afl
    - pdf @ <function>
    - s <address>
    - V
    - pdd @ <address>
    - iz
    - izz
    - izzq
    - axt <address>
    - afn <name>
    - afu <pattern>
    - afll
    - db <address>
    - dc
    - dr
    - Vpp
    - wox <value> @ <address>
    - q

JUST
MOBILE
SECURITY

Android & iOS Cheatsheet

Frida

$frida-ps -U
Lists all running processes on the connected Android device. (Displays process names and their corresponding process identifiers (PIDs).)

$frida -U -f package_name
Attaches to a running process for dynamic analysis.

$frida -U -l script.js -f package_name
Injects and runs a Frida script into the specified package for dynamic analysis.

$frida-trace -U -f package_name -m "-[Class method]"
Traces a specific method of a class for detailed analysis.

$frida-trace -U -f package_name -i "function_name"
Traces a specific function for detailed analysis.

$frida-kill -U package_name
Terminates the specified package forcefully.

$frida-memdump -U -f package_name -O output_file
Dumps the memory of a specific process to a file.

$frida-discover
Discovers and lists nearby Frida server devices.

$frida-server -l 0.0.0.0:27042
Starts the Frida server on a specific host and port for remote device communication.

Nuclei

$ nuclei -list-templates
Lists all available Nuclei templates.
$ nuclei -t <template> -u <target>
Runs a specific template against a target URL.
$ nuclei -t <template> -l <target_file>
Runs a specific template against a list of targets from a file.
$ nuclei -t <template> -u <target> -o <output_file>
Saves the results of a scan to a specified output file.

$ nuclei -t <template> -u <target> -severity <severity>
Filters templates based on the specified severity level.
$ nuclei -t <template> -u <target> -tags <category>
Filters templates based on the specified category.
$ nuclei -t <template> -u <target> -proxy <proxy_url>
Sets the proxy URL for making requests.
$ nuclei -t <template> -u <target> -v
Enables verbose output for detailed scanning information.

R2 (Radare)

r2 <file>
Opens the specified file in Radare2 for analysis.
aaa
Analyzes the binary, performing several automated analysis tasks, such as function detection, basic block identification, and more.
afl
Lists all functions in the binary.
pdf @ <function>
Disassembles the specified function and displays it in the default output format.
s <address>
Seeks to the specified address in the binary.

axt <address>
Cross-references the specified address, showing all references to it.
afn <name>
Searches for a function with the specified name.
afu <pattern>
Searches for functions matching the specified pattern.
afll
Lists all local variables for the current function.
db <address>
Sets a breakpoint at the specified address.

V
Enters the visual mode, providing an interactive interface for exploring and analyzing the binary.
pdd @ <address>
Disassembles the data at the specified address.
iz
Lists all strings found in the binary.
izz
Lists all function names and strings found in the binary.
izzq
Lists all unique function names found in the binary.

dc
Continues the execution after a breakpoint or stops.
dr
Shows all registers and their values.
Vpp
Opens the pseudo-graph view to visualize the control flow graph.
wox <value> @ <address>
Overwrites the value at the specified address with the specified value.
q
Quits Radare2.

JUST
MOBILE
SECURITY