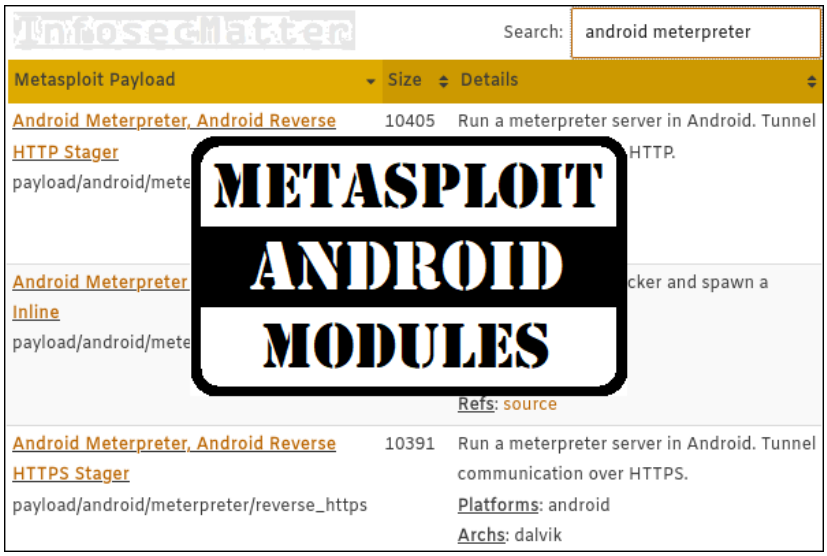
Metasploit Android Modules

infosecmatter.com/metasploit-android-modules

June 5, 2021



On this page you will find a comprehensive list of all **Metasploit Android modules** that are currently available in the latest Metasploit Framework, the most popular penetration testing platform.

I'm hoping that this list will help you find the right modules for pentesting of Android devices with Metasploit.

Introduction

There are more than 4,280 different modules in the latest Metasploit Framework (version v6.0.44-dev), supporting more than 33 different operating system platforms and 30 different processor architectures. Android (dalvik) is of course also supported.

In total, there are 52 Metasploit modules either directly for Android devices (e.g. `exploit/android/..`), or indirectly affecting Android platform as they support either Android OS or the Dalvik architecture (e.g. `exploit/multi/..`).

Here's a breakdown of all Metasploit modules that can be used on Android devices:

- 8 exploits and 9 payloads
- 7 privilege escalation exploits
- 12 post exploitation modules
- 16 auxiliary modules

You can find the complete list of these modules in the following section. For better overview, you can see more detailed information in the spreadsheets section further down below.

Metasploit Android modules (overview)

Here is the actual list of all Metasploit modules that can be used on Android devices. Clicking on the modules will let you see a detailed information about each module.

1. Metasploit exploits for Android:

2. Metasploit privilege escalation exploits for Android:

3. Metasploit payloads for Android:

4. Metasploit post exploitation modules for Android:

5. Metasploit auxiliary modules for Android:

See the spreadsheets section further down below for much more detailed list overview.

Android Meterpreter commands

When it comes to pentesting on Android platform, one of the strong points of Metasploit is the Android Meterpreter.

Once you establish a meterpreter shell session with your target Android device, there are many powerful and useful built-in commands that allow you to control the device.

Here’s a full list of all meterpreter android shell commands:

```
[*] Sending stage (77012 bytes) to 10.10.24.1
[*] Meterpreter session 1 opened (10.10.10.3:4444 -> 10.10.24.1:50619) at 2021-06-04 02:40:02

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    upload        Upload a file or directory


Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

```
Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getuid        Get the user that the server is running as
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS


Stdapi: User interface Commands
===============================

    Command       Description
    -------       -----------
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Android Commands
================

    Command           Description
    -------           -----------
    activity_start    Start an Android activity from a Uri string
    check_root        Check if device is rooted
    dump_calllog      Get call log
    dump_contacts     Get contacts list
    dump_sms          Get sms messages
    geolocate         Get current lat-long using geolocation
    hide_app_icon     Hide the app icon from the launcher
    interval_collect  Manage interval collection capabilities
    send_sms          Sends SMS from target session
    set_audio_mode    Set Ringer Mode
    sqlite_query      Query a SQLite database from storage
    wakelock          Enable/Disable Wakelock
    wlan_geolocate    Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command        Description
    -------        -----------
    app_install    Request to install apk file
    app_list       List installed apps in the device
    app_run        Start Main Activty for package name
    app_uninstall  Request to uninstall application

meterpreter >
```

As you can see, there are some very powerful functionalities which allow you to practically take a full control over the device.

You can access the contact directory, send and receive SMS messages, view call history, record audio using the microphone or video using the camera, and even see what's going on on the display.

A common way how you can test it and play with it is by installing Android emulator on your PC and building a malicious APK file using Metasploit msfvenom. Here is a very good tutorial that walks you though the process step by step how to establish a meterpreter session with your Android device:

> https://resources.infosecinstitute.com/topic/lab-hacking-an-android-device-with-msfvenom/

Go back to menu.

Metasploit Android modules (detailed)

This section contains a detailed overview of all those 52 Metasploit Android modules, organized in interactive tables (spreadsheets) with the most important information about each module:

- Module name with a brief description of the module
- List of platforms and CVEs (if specified in the module)
- Reference links in the module providing more details

You can also use the search feature to quickly filter out relevant modules and sort the columns as needed.

Metasploit Android exploits

Here's a detailed list of all Metasploit Android exploits:

Metasploit Module	Date	Rank	Details
Rapid7 Metasploit Framework msfvenom APK Template Command Injection exploit/unix/fileformat/metasploit_msfvenom_apk_template_cmd_injection	2020-10-29	excellent	This module exploits a command injection vulnerability in Metasploit Framework's msfvenom payload generator when using a crafted APK file as an Android payload template. Affects Metasploit Framework ... **Platforms**: unix **CVEs**: CVE-2020-7384 **Refs**: source, ref1
Adobe Reader for Android addJavascriptInterface Exploit exploit/android/fileformat/adobe_reader_pdf_js_interface	2014-04-13	good	Adobe Reader versions less than 11.2.0 exposes insecure native interfaces to untrusted javascript in a PDF. This module embeds the browser exploit from android/webview_addjavascriptinterface into a ... **Platforms**: android **CVEs**: CVE-2014-0514 **Refs**: source
Android Stagefright MP4 tx3g Integer Overflow exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	This module exploits an integer overflow vulnerability in the Stagefright Library (libstagefright.so). The vulnerability occurs when parsing specially crafted MP4 files. While a wide variety of ... **Platforms**: linux **CVEs**: CVE-2015-3864 **Refs**: source, ref1, ref2, ref3, ref4, ref5, ref6, ref7
Samsung Galaxy KNOX Android Browser RCE exploit/android/browser/samsung_knox_smdm_url	2014-11-12	excellent	A vulnerability exists in the KNOX security component of the Samsung Galaxy firmware that allows a remote webpage to install an APK with arbitrary permissions by abusing the 'smdm://' protocol ... **Platforms**: android **Refs**: source, ref1
Android ADB Debug Server Remote Payload Execution exploit/android/adb/adb_server_exec	2016-01-01	excellent	Writes and spawns a native payload on an android device that is listening for adb debug messages. **Platforms**: linux **Refs**: source

Metasploit Module	Date	Rank	Details
Android Janus APK Signature bypass exploit/android/local/janus	2017-07-31	manual	This module exploits CVE-2017-13156 in Android to install a payload into another application. The payload APK will have the same signature and can be installed as an update, preserving the existing ... **Platforms**: android **CVEs**: CVE-2017-13156 **Refs**: source, ref1, ref2
Steamed Hams exploit/multi/hams/steamed	2018-04-01	manual	but it's a Metasploit Module. **Platforms**: android, apple_ios, bsd, java, js, linux, mainframe, multi, nodejs, osx, php, python, ruby, solaris, unix, win **Refs**: source, ref1
Generic Payload Handler exploit/multi/handler	-	manual	This module is a stub that provides all of the features of the Metasploit payload system to exploits that have been launched outside of the framework. **Platforms**: android, apple_ios, bsd, java, js, linux, mainframe, multi, nodejs, osx, php, python, ruby, solaris, unix, win **Refs**: source

Go back to menu.

Metasploit Android privilege escalation exploits

Here's a detailed list of all Android privilege escalation exploits in Metasploit:

Metasploit Module	Date	Rank	Details
Android Browser and WebView addJavascriptInterface Code Execution exploit/android/browser/webview_addjavascriptinterface	2012-12-21	excellent	This module exploits a privilege escalation issue in Android < 4.2's WebView component that arises when untrusted Javascript code is executed by a WebView that has one or more Interfaces added to it. ... **Platforms**: android, linux **CVEs**: CVE-2012-6636, CVE-2013-4710 **Refs**: source, ref1, ref2, ref3, ref4, ref5
Multi Recon Local Exploit Suggester post/multi/recon/local_exploit_suggester	-	normal	This module suggests local meterpreter exploits that can be used. The exploits are suggested based on the architecture and platform that the user has a shell opened as well as the available exploits ... **Platforms**: all **Refs**: source, docs
Allwinner 3.4 Legacy Kernel Local Privilege Escalation exploit/multi/local/allwinner_backdoor	-	excellent	This module attempts to exploit a debug backdoor privilege escalation in Allwinner SoC based devices. Vulnerable Allwinner SoC chips: H3, A83T or H8 which rely on Kernel 3.4 Vulnerable OS: all OS ... **CVEs**: CVE-2016-10225 **Refs**: source
Android get_user/put_user Exploit exploit/android/local/put_user_vroot	2013-09-06	excellent	This module exploits a missing check in the get_user and put_user API functions in the linux kernel before 3.5.5. The missing checks on these functions allow an unprivileged user to read and write ... **CVEs**: CVE-2013-6282 **Refs**: source, ref1, ref2, ref3
Android 'Towelroot' Futex Requeue Kernel Exploit exploit/android/local/futex_requeue	2014-05-03	excellent	This module exploits a bug in futex_requeue in the Linux kernel, using similar techniques employed by the towelroot exploit. Any Android device with a kernel built before June 2014 is likely to be ... **Platforms**: android, linux **CVEs**: CVE-2014-3153 **Refs**: source, ref1, ref2

Metasploit Module	Date	Rank	Details
Android Binder Use-After-Free Exploit exploit/android/local/binder_uaf	2019-09-26	excellent	This module exploits CVE-2019-2215, which is a use-after-free in Binder in the Android kernel. The bug is a local privilege escalation vulnerability that allows for a full compromise of a vulnerable ... **Platforms**: android, linux **CVEs**: CVE-2019-2215 **Refs**: source, ref1, ref2, ref3, ref4
Android 'su' Privilege Escalation exploit/android/local/su_exec	2017-08-31	manual	This module uses the su binary present on rooted devices to run a payload as root. A rooted Android device will contain a su binary (often linked with an application) that allows the user to run ... **Platforms**: android, linux **Refs**: source

Go back to menu.

Metasploit Android payloads

Here's a detailed list of all Android payloads in Metasploit:

Metasploit Payload	Size	Details
Android Meterpreter, Android Reverse HTTP Stager payload/android/meterpreter/reverse_http	10405	Run a meterpreter server in Android. Tunnel communication over HTTP. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse HTTP Inline payload/android/meterpreter_reverse_http	79840	Connect back to attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter, Android Reverse HTTPS Stager payload/android/meterpreter/reverse_https	10391	Run a meterpreter server in Android. Tunnel communication over HTTPS. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse HTTPS Inline payload/android/meterpreter_reverse_https	79789	Connect back to attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter, Android Reverse TCP Stager payload/android/meterpreter/reverse_tcp	10173	Run a meterpreter server in Android. Connect back stager. **Platforms**: android **Archs**: dalvik **Refs**: source
Android Meterpreter Shell, Reverse TCP Inline payload/android/meterpreter_reverse_tcp	79571	Connect back to the attacker and spawn a Meterpreter shell. **Platforms**: android **Archs**: dalvik **Refs**: source
Command Shell, Android Reverse HTTP Stager payload/android/shell/reverse_http	10439	Spawn a piped command shell (sh). Tunnel communication over HTTP. **Platforms**: android **Archs**: dalvik **Refs**: source
Command Shell, Android Reverse HTTPS Stager payload/android/shell/reverse_https	10288	Spawn a piped command shell (sh). Tunnel communication over HTTPS. **Platforms**: android **Archs**: dalvik **Refs**: source
Command Shell, Android Reverse TCP Stager payload/android/shell/reverse_tcp	10156	Spawn a piped command shell (sh). Connect back stager. **Platforms**: android **Archs**: dalvik **Refs**: source

Go back to menu.

Metasploit Android post exploitation modules

Here's a detailed list of all Android post exploitation modules in Metasploit:

Metasploit Module	Date	Details
Multiplatform Installed Software Version Enumerator post/multi/gather/enum_software_versions	-	This module, when run against a compromised machine, will gather details on all installed software, including their versions and if available, when they were installed, and will save it into a loot ... **Platforms**: android, bsd, linux, osx, solaris, win **Refs**: source, docs
Android Root Remove Device Locks (root) post/android/manage/remove_lock_root	-	This module uses root privileges to remove the device lock. In some cases the original lock method will still be present but any key/gesture will unlock the device. **Platforms**: android **Refs**: source, docs
Multiplatform WLAN Enumeration and Geolocation post/multi/gather/wlan_geolocate	-	Enumerate wireless networks visible to the target device. Optionally geolocate the target by gathering local wireless networks and performing a lookup against Google APIs. **Platforms**: android, bsd, linux, osx, solaris, win **Refs**: source, docs
Android Settings Remove Device Locks (4.0-4.3) post/android/manage/remove_lock	2013-10-11	This module exploits a bug in the Android 4.0 to 4.3 com.android.settings.ChooseLockGeneric class. Any unprivileged app can exploit this vulnerability to remove the lockscreen. A logic flaw / design ... **Platforms**: android **CVEs**: CVE-2013-6271 **Refs**: source, ref1, ref2
Displays wireless SSIDs and PSKs post/android/gather/wireless_ap	-	This module displays all wireless AP creds saved on the target device. **Platforms**: android **Refs**: source, docs
Multi Manage Set Wallpaper post/multi/manage/set_wallpaper	-	This module will set the desktop wallpaper background on the specified session. The method of setting the wallpaper depends on the platform type. **Platforms**: android, linux, osx, win **Refs**: source
Multi Manage YouTube Broadcast post/multi/manage/play_youtube	-	This module will broadcast a YouTube video on specified compromised systems. It will play the video in the target machine's native browser. The VID datastore option is the "v" parameter in a YouTube ... **Platforms**: android, linux, osx, unix, win **Refs**: source, docs
Android Gather Dump Password Hashes for Android Systems post/android/gather/hashdump	-	Post Module to dump the password hashes for Android System. Root is required. To perform this operation, two things are needed. First, a password.key file is required as this contains the hash but no ... **Platforms**: android **Refs**: source, docs, ref1, ref2
extracts subscriber info from target device post/android/gather/sub_info	-	This module displays the subscriber info stored on the target phone. It uses call service to get values of each transaction code like imei etc. **Platforms**: android **Refs**: source, docs
Android Screen Capture post/android/capture/screen	-	This module takes a screenshot of the target phone. **Platforms**: android **Refs**: source, docs
Multi Manage Network Route via Meterpreter Session post/multi/manage/autoroute	-	This module manages session routing via an existing Meterpreter session. It enables other modules to 'pivot' through a compromised host when connecting to the named NETWORK and SUBMASK. Autoadd will ... **Refs**: source, docs
KOFFEE - Kia OFFensivE Exploit post/android/local/koffee	2020-12-02	This module exploits CVE-2020-8539, which is an arbitrary code execution vulnerability that allows an to attacker execute the micomd binary file on the head unit of Kia Motors. This module has been ... **CVEs**: CVE-2020-8539 **Refs**: source, docs, ref1

Go back to menu.

Metasploit Android auxiliary modules

Here's a detailed list of all Android auxiliary modules in Metasploit:

Metasploit Module	Date	Details

Metasploit Module	Date	Details
Android Browser RCE Through Google Play Store XFO auxiliary/admin/android/google_play_store_uxss_xframe_rce	-	This module combines two vulnerabilities to achieve remote code execution on affected Android devices. First, the module exploits CVE-2014-6041, a Universal Cross-Site Scripting (UXSS) vulnerability ... **CVEs**: CVE-2014-6041 **Refs**: source, ref1, ref2
Android Browser "Open in New Tab" Cookie Theft auxiliary/gather/android_browser_new_tab_cookie_theft	-	In Android's stock AOSP Browser application and WebView component, the "open in new tab" functionality allows a file URL to be opened. On versions of Android before 4.4, the path to the sqlite cookie ... **Refs**: source, ref1, ref2
Android Stock Browser Iframe DOS auxiliary/dos/android/android_stock_browser_iframe	2012-12-01	This module exploits a vulnerability in the native browser that comes with Android 4.0.3. If successful, the browser will crash after viewing the webpage. **CVEs**: CVE-2012-6301 **Refs**: source
ES File Explorer Open Port auxiliary/scanner/http/es_file_explorer_open_port	2019-01-16	This module connects to ES File Explorer's HTTP server to run certain commands. The HTTP server is started on app launch, and is available as long as the app is open. Version 4.1.9.7.4 and below are ... **CVEs**: CVE-2019-6447 **Refs**: source, docs, ref1, ref2, ref3
Android Open Source Platform (AOSP) Browser UXSS auxiliary/gather/android_object_tag_webview_uxss	2014-10-04	This module exploits a Universal Cross-Site Scripting (UXSS) vulnerability present in all versions of Android's open source stock browser before 4.4, and Android apps running on < 4.4 that embed the ... **Refs**: source, ref1, ref2, ref3
Android Meterpreter Browsable Launcher auxiliary/server/android_browsable_msf_launch	-	This module allows you to open an android meterpreter via a browser. An Android meterpreter must be installed as an application beforehand on the target device in order to use this. For best results, ... **Refs**: source, ref1
Android Browser File Theft auxiliary/gather/android_browser_file_theft	-	This module steals the cookie, password, and autofill databases from the Browser application on AOSP 4.3 and below. **Refs**: source, ref1, ref2
Samsung Internet Browser SOP Bypass auxiliary/gather/samsung_browser_sop_bypass	2017-11-08	This module takes advantage of a Same-Origin Policy (SOP) bypass vulnerability in the Samsung Internet Browser, a popular mobile browser shipping with Samsung Android devices. By default, it ... **CVEs**: CVE-2017-17692 **Refs**: source, docs, ref1
Android Open Source Platform (AOSP) Browser UXSS auxiliary/gather/android_stock_browser_uxss	-	This module exploits a Universal Cross-Site Scripting (UXSS) vulnerability present in all versions of Android's open source stock browser before 4.4, and Android apps running on < 4.4 that embed the ... **CVEs**: CVE-2014-6041 **Refs**: source, ref1
Android Content Provider File Disclosure auxiliary/gather/android_htmlfileprovider	-	This module exploits a cross-domain issue within the Android web browser to exfiltrate files from a vulnerable device. **CVEs**: CVE-2010-4804 **Refs**: source, ref1
Android Mercury Browser Intent URI Scheme and Directory Traversal Vulnerability auxiliary/server/android_mercury_parseuri	-	This module exploits an unsafe intent URI scheme and directory traversal found in Android Mercury Browser version 3.2.3. The intent allows the attacker to invoke a private wifi manager activity, ... **Refs**: source, ref1, ref2
Firefox PDF.js Browser File Theft auxiliary/gather/firefox_pdfjs_file_theft	-	This module abuses an XSS vulnerability in versions prior to Firefox 39.0.3, Firefox ESR 38.1.1, and Firefox OS 2.2 that allows arbitrary files to be stolen. The vulnerability occurs in the PDF.js ... **CVEs**: CVE-2015-4495 **Refs**: source, ref1, ref2, ref3

Metasploit Module	Date	Details
SIPDroid Extension Grabber auxiliary/scanner/sip/sipdroid_ext_enum	-	This module exploits a leak of extension/SIP Gateway on SIPDroid 1.6.1 beta, 2.0.1 beta, 2.2 beta (tested in Android 2.1 and 2.2 - official Motorola release) (other versions may be affected). **Refs**: source, ref1
HTTP Client Automatic Exploiter 2 (Browser Autopwn) auxiliary/server/browser_autopwn2	2015-07-05	This module will automatically serve browser exploits. Here are the options you can configure: The INCLUDE_PATTERN option allows you to specify the kind of exploits to be loaded. For example, if you ... **Refs**: source, docs, ref1
HTTP Client Automatic Exploiter auxiliary/server/browser_autopwn	-	This module has three actions. The first (and the default) is 'WebServer' which uses a combination of client-side and server-side techniques to fingerprint HTTP clients and then automatically exploit ... **Refs**: source
Password Cracker: Mobile auxiliary/analyze/crack_mobile	-	This module uses Hashcat to identify weak passwords that have been acquired from Android systems. These utilize MD5 or SHA1 hashing. Android (Samsung) SHA1 is format 5800 in Hashcat. Android ... **Refs**: source, docs

Go back to menu.

See also

- Metasploit Windows Exploits (Detailed Spreadsheet)
- Metasploit Linux Exploits (Detailed Spreadsheet)
- Metasploit Auxiliary Modules (Detailed Spreadsheet)
- Post Exploitation Metasploit Modules (Reference)
- Metasploit Payloads (Detailed Spreadsheet)
- Metasploit Module Library

TAGS | Android | Auxiliary | CVE | Dalvik | Denial-of-service | Exploitation | Metasploit | Meterpreter | Msfconsole | Payload | Post-exploitation | Privilege escalation | RCE | Spreadsheet