

REMNUX USAGE TIPS FOR MALWARE ANALYSIS ON LINUX

This cheat sheet outlines the tools and commands for analyzing malicious software on [REMnux Linux distro](#).

Getting Started with REMnux

Download REMnux as a virtual appliance or install the distro on an existing compatible system, such as [SIFT](#).

Log into the REMnux virtual appliance as the user “remnux”, default password “malware”.

Use apt-get to install additional software packages if your system is connected to the Internet.

Run the update-remnux command to upgrade REMnux and update its software.

Switch keyboard layout by clicking the keyboard icon in the bottom right corner of the REMnux desktop.

On VMware, install VMware Tools using install-vmware-tools to adjust the screen size.

General Commands on REMnux

Shut down the system	shutdown
Reboot the system	reboot
Switch to a root shell	sudo -s
Renew DHCP lease	renew-dhcp
See current IP address	myip
Edit a text file	scite <i>file</i>
View an image file	feh <i>file</i>
Start web server	httpd start
Start SSH server	sshd start

Statically Examine Files

Inspect file properties using [pescanner](#), [pestr](#), [pyew](#), [readpe](#), [pedump](#), [peframe](#), [signsrch](#), [readpe.py](#).

Investigate binary files in-depth using [bokken](#), [vivbin](#), [udcli](#), [RATDecoders](#), [radare2](#), [yara](#), [wxHexEditor](#).

Deobfuscate contents with [xorsearch](#), [unxor.py](#), [Balbuzard](#), [NoMoreXOR.py](#), [brutexor.py](#), [xortool](#).

Examine memory snapshots using [Rekall](#), [Volatility](#).

Assess packed files using [densityscout](#), [bytehist](#), [packerid](#), [upx](#).

Extract and carve file contents using [hachoir-subfile](#), [bulk_extractor](#), [scalpel](#), [foremost](#).

Scan files for malware signatures using [clamscan](#) after refreshing signatures with [freshclam](#).

Examine and track multiple malware samples with [mas](#), [viper](#), [malttrieve](#), [Ragpicker](#).

Work with file hashes using [nsrlookup](#), [Automater](#), [hash_id](#), [ssdeep](#), [totalhash](#), [virustotal-search](#), [vt](#).

Define signatures with [yaraGenerator.py](#), [autorule.py](#), [IOCextractor.py](#), [rule-editor](#).

Handle Network Interactions

Analyze network traffic with [wireshark](#), [ngrep](#), [tcpick](#), [tcpxtract](#), [tcpflow](#), [tcpdump](#).

Intercept all laboratory traffic destined for IP addresses using accept-all-ips.

Analyze web traffic with [burpsuite](#), [mitmproxy](#), [CapTipper](#), [NetworkMiner](#).

Implement common network services using [fakedns](#), [fakesmtp](#), [inetsim](#), “ircd start”, “httpd start”.

Examine Browser Malware

Deobfuscate JavaScript with [SpiderMonkey](#) (js), [d8](#), [rhino-debugger](#) and [Firebug](#).

Define JavaScript objects for SpiderMonkey using /usr/share/remnux/objects.js.

Clean up JavaScript with [js-beautify](#).

Retrieve web pages with wget and curl.

Examine malicious Flash files with [swfdump](#), [flare](#), [RABCDasm](#), [xxxswf.py](#), [extract_swf](#).

Analyze Java malware using [idx_parser.py](#), [cfr](#), [jad](#), [jd-gui](#), [Javassist](#).

Inspect malicious websites and domains using [thug](#), [Automater](#), [pdnstool.py](#), [passive.py](#).

Examine Document Files

Analyze suspicious Microsoft Office documents with [officeparser.py](#), [oletools](#), [libolecf](#), [oledump.py](#).

Examine PDFs using [pdfid](#), [pdfwalker](#), [pdf-parser](#), [pdfdecompress](#), [pdfxray_lite](#), [pyew](#), [peepdf](#).

Extract JavaScript or SWFs from PDFs using “pdfextract”, “pdf.py” and [swf_mastah](#).

Examine shellcode using [shellcode2exe.py](#), [sctest](#), [dism-this](#), [unicode2hex-escaped](#), [m2elf](#), [dism-this.py](#).

Investigate Linux Malware

Disassemble and debug binaries using [bokken](#), [vivbin](#), [edb](#), [gdb](#), [udcli](#), [radare2](#), [objdump](#).

Examine the system during behavioral analysis with [sysdig](#), [unhide](#), [strace](#), [ltrace](#).

Examine memory snapshots using [Rekall](#), [Volatility](#).

Decode Android malware using [Androwarn](#), [AndroGuard](#).

Examine Memory Using Volatility

Determine profile	kdbgscan, imageinfo
Spot hidden processes	psxview
List all processes	pslist, psscan
Show a registry key	printkey -K key
Extract process image	procdump
Extract process memory	memdump, vaddump
List open handles, files, DLLs and mutant objects	handles, filescan, dlllist, mutantscan
List services, drivers and kernel modules	svcsan, driverscan, modules, modscan
View network activities	connscan, connections, sockets, sockscan, netscan
View activity timeline	timeliner, evtlogs
Find and extract malware	malfind, apihooks

Additional Resources

[REMnux Documentation](#)

[Reverse-Engineering Malware Cheat Sheet](#)

[Analyzing Malicious Documents Cheat Sheet](#)

[SANS Reverse-Engineering Malware Course](#)