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 from REMnux.org as a Live CD ISO image file or a VMware/VirtualBox virtual appliance.

Operate in REMnux as the user “remnux”. The default password for this account is “malware”.

Run privileged commands on REMnux using “sudo”.

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

Use “setxkbmap” to switch keyboard layout. For example, for German layout use “setxkbmap de”.

You can switch the screen resolution using “xrandr” followed by the “xrandr -s” command.

If using VMware, you can install VMware Tools to automatically adjust the screen size.

General Commands for Using 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 *file*
View an image file	feh *file*
Start web server	httpd start
Start SSH server	sshd start

Analyzing Network Malware

For IRC bots, start the IRC daemon (“ircd start”) and the IRC client (“irc”).

Analyze network traffic with “wireshark”, “ngrep” “tcpdump”, “pdnstool”, “NetworkMiner” and “nc”.

Intercept traffic and emulate some services with Honeyd (“farpd start”, then “honeyd start”).

Emulate common network services using “fakedns”, “fakesmtp” and “inetsim”.

Wrap network traffic with SSL using “stunnel”.

Examining Malicious Websites

Deobfuscate JavaScript with SpiderMonkey (“js”), “d8”, “rhino-debugger” and Firebug.

Define JavaScript objects using /usr/local/etc/def.js.

You can clean up JavaScript with “js-beautify”.

Control web traffic with “burpsuite”, Tamper Data.

Retrieve websites with “wget” and “curl”.

Hide your origin with “tor start”, “usewithtor”.

Examine malicious Flash files with “swfdump -Ddu”, “flare”, RABCDAsm, and “xxxswf.py”.

Inspect malicious websites and traffic captures with “jsunpackn” after “cd ~remnux/jsunpackn”.

Analyzing Malicious Document Files

Examine suspicious Microsoft Office documents with “pyOLEScanner.py” and “hachoir-urwid”.

Navigate through PDFs using “pyew”, “peepdf” and “pdfwalker”.

Extract JavaScript or SWFs from PDFs using “pdfextract”, “pdf.py” and “swf_mastah”.

Examine PDFs using “pdfcop”, “pdf-parser”, “pdfid”, “pdfdecompress” and “pdfxray_lite”.

Emulate shellcode execution using “sctest -Svs”.

Analyzing Executables and Other Files

Scan the executable for suspicious characteristics and packer signatures using “pescanner”.

Check whether the file might be packed using “densityscout” and “bytehist”.

Explore the executable’s internals using “pyew”.

Identify file type using “trid” and “file”.

Scan files for malware signatures using “clamscan” after refreshing signatures with “sudo freshclam”.

Disassemble code using “radare”, “pyew”, “gdb” and “objdump -Mintel -D”.

Extract metadata using “hachoir-metadata”.

Find and extract subfiles using “hachoir-subfile”.

Compare binary files using “vbindiff”.

Find obfuscated or encrypted data with “xorsearch”, “findaes”, “xortool”, “aeskeyfind”, “rsakeyfind”.

Decompile Java class files using “jad” and “jd-gui”.

Analyze memory image files using “volatility”.

Volatility Memory Forensics Commands

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

Useful Configuration Files on REMnux

Honeyd	/etc/honeypot/honeyd.conf
INetSim	/etc/inetsim/inetsim.conf
Web server	/etc/thttpd/thttpd.conf
IRC server	/etc/inspircd/inspircd.conf
SSH server	/etc/ssh/sshd_config
Aliases	~remnux/.bash_aliases
Wget	~remnux/.wgetrc

References

Reverse-Engineering Malware Cheat Sheet

Analyzing Malicious Documents Cheat Sheet

SANS Reverse-Engineering Malware Course

Authored by Lenny Zeltser for REMnux v3. Lenny writes a security blog at blog.zeltser.com and is active on Twitter as @lennyzeltser. Such malware analysis topics are covered in Lenny’s Reverse-Engineering Malware (REM) course, which he teaches at SANS Institute—for details visit LearnREM.com.