REMnux Manual

Table of Contents

Introduction to REMnux

REMnux is a special Linux distribution, specifically designed for malware analysis, reverse engineering and forensic investigations. It is developed and maintained by Lenny Zeltser, CISO at Axonius. REMnux is kitted out with an array of tools that are tailored to assist security researchers, analysts and incident responders in examining malware, suspicious files and network traffic.

Minimum System Requirements

- **CPU:** 64-bit processor (x86_64 architecture)
- **RAM:** Min. 2 GB – Recommended 4 GB
- **Disk Space:** Min. 20 GB – Recommended 40 GB
- **GPU:** Standard graphics support sufficient for running a desktop environment.
- **Network:** Active network connection

REMnux has some key features such as

1. Malware Analysis
2. Reverse Engineering
3. Network Analysis
4. Forensics
5. Utilities and Frameworks

Advantages of using REMnux

1. Comprehensive Tools

   REMnux bundles a wide range of tools into one distribution, making it easier for analysts to have everything they need in a single environment.

2. Ease of use

   Pre-configured and ready to use tools save time and effort in setting up an analysis environment.

3. Regular updates

   The distribution is regularly updated to include the latest tools and improvements, ensuring that analysts have access to the most current resources.

4. Community support

   REMnux has a strong community of users and contributors, providing support, sharing knowledge and collaborating on imporiving the distribution.

5. Documentation and training

   Comprehensive training resources and documentation are available to help users get started and make the most of the tools included in REMnux.

Installation of REMnux

Now let's go over the installation process of REMnux. It will be pretty compact, as it is a straight forward process.

1. Download the REMnux OVA file

   - Go over to the official REMnux website and download the latest version.

2. Import the OVA file into your virtualization software

   - Open your virtualization software, in my case I'm using VirtualBox.
   - Import the OVA file
   - For VirtualBox: Go to 'File' > 'Import Appliance' > Select the downloaded OVA file > Follow the prompts.
   - For VMware: Go to 'File' > 'Open' > Select the downloaded OVA file > Follow the prompts.

3. Configure the VM settings

   - Adjust the VM settings as needed. Allocate more RAM, change network settings,...

4. Start the VM

   - Start the VM and complete any initial setup prompts.

In case you want to install REMnux on an existing Ubuntu VM, please follow the instructions. If not, you can skip this part.

1. Create and set up an Ubuntu VM

   - Download the latest Ubuntu LTS ISO from the Ubuntu website
   - Open your favorite virtualization software and create a new VM
   - For VirtualBox or VMware : Create a new VM and select the Ubuntu ISO as the installation media.
   - Follow the prompts to install Ubuntu on the VM.

2. Update the Ubuntu system:

   ‘sudo apt update && sudo apt upgrade -y’

3. Install REMnux:

   ‘wget -O – https://remnux.org/get-remnux.sh | sudo bash’
   - Follow the on-screen instructions to complete the installation.

4. Reboot the VM:

   ‘sudo reboot’

Included Tools

REMnux includes a vast array of tools for malware analysis, reverse engineering, network analysis and digital forensics. I listed all included tools down below.

Malware Analysis Tools

1. Binary Analysis

- Ghidra: A software reverse engineering framework developed by the NSA.
- Radare2: A free and open-source reverse engineering framework.
- IDA Free: A free version of the Interactive Disassembler.
- OllyDbg: An x86 debugger that emphasizes binary code analysis.

2. Static Analysis

- strings: Displays printable strings in a binary file.
- exiftool: Reads, writes, and manipulates metadata in files.
- hexedit: A hexadecimal file editor.
- peframe: A tool to analyze Portable Executable files.
- Binwalk: Analyzes and extracts firmware images.

3. Dynamic Analysis

- Cuckoo Sandbox: An automated malware analysis system.
- INetSim: A software suite for simulating common internet services to analyze malware.
- Wireshark: A network protocol analyzer.

4. File Analysis

- YARA: Identifies and classifies malware samples.

- VirusTotal Tools: Tools for interacting with the VirusTotal API to scan files against a database of known malware.

- OLETools: A package for analyzing Microsoft OLE2 files.

Reverse Engineering Tools

1. Disassemblers and Debuggers

- Ghidra: Analyzes binary code and decompiles it into a high-level representation.

- Radare2: Performs binary analysis and reverse engineering.

- OllyDbg: Debugs and disassembles x86 binaries.

2. Decompilers

- Decompiler Explorer: Allows browsing and comparing multiple decompiled versions of binaries.

3. Hex Editors

- hexedit: Edits binary files at the byte level.

Network Analysis Tools

1. Traffic Analysis

- tcpdump: Captures and analyzes network packets.

- Wireshark: A network protocol analyzer for deep inspection of network traffic.

- NetworkMiner: A network forensic analysis tool.

2. Network Simulation

- INetSim: Simulates various internet services for analyzing malware behavior.

Forensic Analysis Tools

1. File System and Memory Analysis

- Volatility: A memory forensics framework for analyzing RAM dumps.
- Autopsy: A digital forensics platform for analyzing hard drives and smartphones.
- Sleuth Kit: A collection of command-line tools for analyzing disk images.

2. Disk Imaging

- Guymager: A forensic imaging tool.
- dc3dd: An enhanced version of GNU dd for digital forensics.

Utility Tools and Frameworks

1. Scripting and Automation

- Python: A versatile programming language for scripting analysis tasks.
- Shell Utilities: Various shell utilities for automating tasks and processing data.

2. Frameworks

- YARA: A pattern-matching tool for malware identification and classification.
- VirusTotal Tools: Interact with the VirusTotal API to check files and URLs against known malware signatures.

Other Tools

1. Document Analysis

- PDFId: Analyzes PDF documents for malicious content.
- pdf-parser: Parses and analyzes PDF files for signs of maliciousness.

2. Network Services

- Honeyd: A small daemon that creates virtual hosts on a network.
- Dionaea: A honeypot for catching malware exploiting vulnerabilities.

3. Web and Script Analysis

- jsunpack-n: A tool for unpacking and analyzing obfuscated JavaScript.

This list covers many of the key tools included in REMnux. The distribution is regularly updated to include new tools and improve existing ones, so the exact list may change over time. For the most up-to-date list and detailed information on each tool, refer to https://docs.remnux.org/ and https://docs.remnux.org/tools/

Sources

This is our brief REMnux manual. For more information regarding updated toolsets, commands and the use of certain tools, please visit the following sources:

REMnux Documentation: https://docs.remnux.org/

REMnux: https://remnux.org/

Ghidra: https://ghidra-sre.org/

Radare2: https://rada.re/n/

IDA Free: https://hex-rays.com/ida-free/

Exiftool: https://exiftool.org/

Binwalk: https://github.com/ReFirmLabs/binwalk

Cuckoo Sandbox: https://cuckoosandbox.org/

INetSim: http://www.inetsim.org/

Wireshark: https://www.wireshark.org/

YARA: https://virustotal.github.io/yara/

VirusTotal: https://www.virustotal.com/

OLETools: https://github.com/decalage2/oletools

tcpdump: http://www.tcpdump.org/

NetworkMiner: http://www.netresec.com/?page=NetworkMiner

Volatility: https://www.volatilityfoundation.org/

Autopsy: https://www.sleuthkit.org/autopsy/

Sleuth Kit: https://www.sleuthkit.org/

Guymager: https://guymager.sourceforge.io/

dc3dd: https://sourceforge.net/projects/dc3dd/

Python: https://www.python.org/

PDFId: https://blog.didierstevens.com/programs/pdf-tools/

Honeyd: http://www.honeyd.org/

Dionaea: https://github.com/DinoTools/dionaea

jsunpack-n: https://code.google.com/archive/p/jsunpack-n/