A Technical Executive Summary on

Malware Analysis using Deep Exploit, REMNux & Cuckoo

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. Malware analysis is further classified into 3 use cases:

- Computer security incident management

In this case, if an organization suspects or discovers some malware into the system, the response teams do malware analysis on the file or selected files. If the analysis confirms the discovery of malware into the system, the response team investigates to determine the impact the malware may have on the internal organization systems.

- Malware research

Researchers observe the behavior of malware to understand the latest tools and technologies used in its construction.

- Incident of Compromise(IOC) extraction:

IOC is a file observed on the network or on an operating system to determine its malicious nature. Vendors of software product companies and cyber specialty companies perform bulk malware analysis in order to determine potential new indicators of compromise.

Deep Exploit

DeepExploit is a fully automated penetration test tool linked with Metasploit.
It has two exploitation modes.

- Intelligence Mode
- Brute-Force Mode

Key Features

- Self-learning
- Efficiently execute exploit
- Deep penetration
- Operation is very easy
- Learning time is very fast

Abilities of Deep Exploit

- Intelligence gathering
- Threat modeling
- Vulnerability analysis
- Exploitation
- Post-Exploitation
- Reporting

REMnux

REMnux is a Linux toolkit for reverse-engineering and analyzing malicious software. It provides a curated collection of free tools created by the community. This is a free Linux toolkit used for reverse-engineering malicious software. It is bundled with various forensic investigation tools. The distro is based on Ubuntu, and it analyses both Linux and Windows-based malware, examining obfuscated code, suspicious documents, etc.

Abilities of REMnux

- Examine suspicious executables, documents, and other artifacts
- Dynamically reverse-engineering of malicious code
- Run memory forensics on an infected host
- Explore network and system interactions for behavioral analysis
- Analyze malicious documents
- Check static properties
- Gather and analyze data
- Static code analysis

Cuckoo

Cuckoo Sandbox is the leading open-source automated malware analysis system. Cuckoo provides a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment. Cuckoo Sandbox is an advanced, extremely modular, and 100% open source automated malware analysis system with infinite application opportunities.

It can retrieve the following type of results:

- Traces of win32 API calls performed by all processes spawned by the malware.
- Files being created, deleted, and downloaded by the malware during its execution.
- Memory dumps of the malware processes.
- Network traffic trace in PCAP format.
- Screenshots of Windows desktop taken during the execution of the malware.
- Full memory dumps of the machines (including automatic running of Volatility).