**MALWARE ANALYSIS USING Deep Exploit, REMNux & Cuckoobox**

Analysis of malware in the simplest terms could be explained as determination of the originality, functioning and Impact that the malicious sample can cause in the system. Analyzing a malware is required so as to enable the organizations to mitigate the chances of backdoor entry as well to make them aware about the vulnerability in the system that a malware can easily use to exploit the environment.

1. CUCKOO SANDBOX

Cuckoo sandbox is one of the leading open source automated malware analysis under windows, macOS, Linux and Android. Cuckoobox basically gives a detailed outline how the files are behaving wrt the context, motivation and breach goals. It analyzes the malicious components involving files such as office documents, emails and executables etc. Cuckoobox enables tracing of API calls as well as the general behavior of the file, further distilling it to the higher-level information being comprehensible to any person. The next advantage of cuckoo is the ability to analyze data even when encryption is carried out using SSL/TLS. Cuckoo further enables you to conduct advanced memory analysis on the infected system via volatility as well as via granularity on process memory using YARA.

The next major advantage of using Cuckoo is the customization it provides, to any aspect in the environmental analysis and further report processing and report formulation. The next plus point being the backening of data, making the process of reverse engineering easier. Providing you the access of formatting even without any licensing requirements.

1. DeepExploit

DeepExploit linked with Metasploit is a fully automated test tool for penetration. Having a positive front for all the opened access ports on the target server; further executing using ML at pinpoint. The next list of features offered by tools, includes: executing exploits at pinpoint via ML. The next important feature being its self-learning power, using reinforcement learning and A3C system, to the target server via RPC API.

The deep penetration offered by DeepExploit targeting not only on the target server but also on the other internal servers. The next plus point being the ability to perform powerful intelligence gathering; identifying the product name with the help of port scanning, machine learning and via content exploration.

Even after being a beta version, DeepExploit can report, analyse and gather intelligence on the malicious contents of the system. The next range of advantage thus, provided by DeepExploit referring first to the pentesters, involves:

* Higher test efficiency.
* Accuracy of the test returned is increased with each use of Deepexploit ( due to the exploitation mechanism involved using ML)

While referring to the benefits, it offers to the Information security officers, the self-vulnerability testing of servers is the gold mark here. The processing flow goes like, gathering intelligence, exploiting it, post-exploitation stage and generation of report, summarizing the vulnerabilities in the system.

1. REMNux

REMNux enables you to detect and analyze malware present on Linux. To begin with install distro on a dedicated system and review the documentations on docs.remnux.org and ensure the system is up to date by periodically checking for updates.

Collection and analyzation of the data comes next in the lane from networks, hashes, files and various other components. Network interactions also needs to explored via monitoring, connecting and service exploring. REMNux enables the reverse engineering so as to analyze the malicious software and being a free tool can help investigation of the malware without even the need to find, configure and installing the tools.