MALWARE ANALYSIS USING DEEP EXPLOIT, REMNUX & CUCKOOBOX

Malware analysis is the process of learning how malware functions and any potential repercussions of a given malware. Malware code can differ radically, and it's essential to know that malware can have many functionalities. These may come in the form of viruses, worms, spyware, and Trojan horses. Each type of malware gathers information about the infected device without the knowledge, or authorization of the user.

The malicious programs provide backdoor entry into computing devices for stealing personal information, confidential data, and much more.

DEEP EXPLOIT

Deep Exploit is fully automated penetration tool linked with Metasploit. Deep Exploit has two exploitation modes.

INTELLIGENCE MODE

Deep Exploit identifies the status of all opened ports on the target server and executes the exploit at pinpoint based on past experience (trained result).

BRUTE FORCE MODE

Deep Exploit executes exploits using all combinations of “exploit module”, “target” and “payload” corresponding to a user’s indicated product name and port number.

Deep Exploit’s key features are following.

EFFICIENTLY EXECUTE REPORTS

If “intelligence mode”, Deep Exploit can execute exploits at pinpoint. If “Brute force mode”, Deep Exploit can execute exploits thoroughly corresponding to user’s indicated product name and port number.

DEEP PENETRATION

If Deep Exploit succeeds the exploit to the target server, it further executes the exploit to other internal servers.

OPERATION IS VERY EASY

Your only operation is to input one command. It is very easy!!

SELF LEARNING

Deep Exploit doesn’t need the “learning data”. Deep Exploit can learn how to method of exploitation by itself.

LEARNING TIME IS VERY FAST

Deep Exploit uses distributed learning by multi-agents.

REMNUX

REMnux is a Linux toolkit for reverse-engineering and analyzing malicious software. REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools.

The REMnux toolkit provides Docker images of popular malware analysis tools that you can run on any compatible system even without installing the REMnux distro.

CUCKOOBOX

Cuckoo Sandbox is the leading open source automated malware analysis system. You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.

Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization. In these evolving times, detecting and removing malware artifacts is not enough: it’s vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach. Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, OS X, Linux, and Android.

Using Cuckoo Sandbox’s open source and highly customizable dynamic malware analysis capabilities, organizations can automate the advanced analysis of malicious and unknown files as part of the automated and orchestrated response to a potential security incident. Cuckoo Sandbox provides critical insights in to the capabilities of a file, providing the basis for additional automated and manual decisions on the appropriate response to an incident.