ABSTRACT

Every year a lot of attacks from a web vulnerability. The attack came from a hacker/hacker. The majority of hackers use the Kali Linux OS (Operating System) to carry out their actions to start attacks. However, what they really need before starting the action is information gathering. One of them is using passive information gathering. Passive information gathering is the first step for hackers to hack a system. Passive information gathering is gathering information on the target as much as possible without establishing direct contact between the tester and the network device on the target. In passive information gathering, with recon-ng which is rich in tools, you can get a collection of passive information on a web. After getting passive information, it is then upgraded to active information gathering. Active information gathering is the second stage of hackers, who will look for vital information from a web that involves sensitive things on a web. Such as, open ports, ports that have a firewall in them, which ports are closed, what version of ports are used on a web, and so on. The point depends on the ports that are open to exploit. In active information gathering, use the nmap tool. Then, after getting sensitive information about a target web, the last step is to look for vulnerabilities in the port against the target web with the aim of exploiting it. Searching for vulnerabilities actually uses many ways. However, the author only describes tools that are often used and available on Kali Linux. The tool is searchsploit/exploitdb. With searchsploit can bring up specific vulnerabilities to exploit on a target web. However, there are actions to mitigate this. One of them is to always update the latest version of the patch on the port that is found to be a vulnerability on a target web.

Keywords: port, web, recon-ng, passive information gathering, vulnerability