ASSIGNMENT-2

KALI TOOLS:

1) INFORMATION GATHERING:

NMAP:

Another frequently used tool is Nmap that is used for network discovery and auditing of security. Options are present, which notifies of each open port available on the target.

WhatWeb:

This utility enables the utility of information gathering and is like a website fingerprint. It is analogous to an interrogation agent who tries to interrogate a website in getting answers to what that website is built of. To help WhatWeb, there are 1800 plugins, each having their own utility.

2)REVERSE ENGINEERING:

Ghidra:

Ghidra is a powerful open-source software reverse engineering tool developed by the NSA. It can be used to analyze binary executables and help you understand their functionality.

IDA Pro:

IDA Pro is a widely used commercial disassembler and debugger that's known for its robust features and capabilities in reverse engineering.

3)WEB APPLICATION ANALYSIS:

BurpSuite: This is another addition to the web application analysis, which itself comprises of a collection of tools that are bundled to form a single suite of web application's security testing starting from the scratch, i.e. analysis of the attack surface.

4) VULNERABILITY ANALYSIS:

Nikto:

One of the common tools used for assessing vulnerability and security threats. This tool has the capability to scan for 6500+ files or programs, which can be potentially dangerous.

5)PASSWORD ATTACKS:

John the Ripper:

Another widely used offline password cracking service that combines a lot of password crackers into a single package. It takes care of identifying the hash type, customization cracker and many such more and that too in offline mode!

6)DATABASE ASSESSMENT:

SQLMap:

This is one of the most widely used tools for database assessment as the process of detection and exploitation of vulnerabilities present in SQL injection, which can lead to taking over of database. For carrying on with this, we might need to find a website that is SQL injection vulnerable, for which another tool discussed above, SQLiv, will come in handy!

7)WIRELESS ATTACK:

Aircrack-NG suite:

As the name suggests that this is a suite, a scanner, WEP and WPA/WPA2-PSK cracker, a packet sniffer and an analysis tool is threaded together to carry out tasks to crack or identify vulnerabilities in any wireless mediums! This tool consists of 16 sub-tools to carry on with the utility.

8)SPOOFING AND SNIFFING:

BetterCAP:

Another great tool for performing man in the middle attacks against a network. This is achieved by manipulation of HTTP, HTTPS, TCP traffic in real-time, credential sniffing and many such more to carry out such attacks!