ServerSide Attacks

Tools in Kali Linux

Module #17

Servers: Introduction

Servers are computer program running to serve the requests of other programs, known as the "clients".
The server performs some computational task on behalf of "clients".
The clients either run on the same computer, or connect through the network.
For example, a server would host a game to the world while clients would access the game remotely. There are various forms of providing services to clients such as an Apache Web Server limited to HTTP or a BEA WebLogic Application Server that does HTTP plus more.

Servers: Introduction (Contd.)

Network servers are typically configured to handle the load of servicing large volumes of clients.

This means adding additional processing, memory and storage making these assets valuable targets for hackers.

Organizations typically manage servers remotely and don't actively monitor activity, meaning small hits in performance or other indicators of being compromised may go unnoticed.

It's common to find malicious users have accessed compromised servers for long periods of time prior to the owners identifying the vulnerability used to access the system.

Servers: Vulnerability Assessment

Server-side attacks are exploiting and finding vulnerabilities in services, ports, and applications running on a server.

For example, a web server has several attack vectors:

- It is a server running an operating system
- It runs various pieces of software to provide web functionality
- It has many open TCP ports.

Each one of these vectors could harvest a vulnerability that an attacker could exploit

Kali Linux: Skipfish tool

Skipfish is a web application security Reconnaissance tool.
Skipfish prepares an interactive sitemap for the target using recursive crawl and dictionary-based probes.

Skipfish can be found under Web Applications | Web Vulnerability Scanners as skipfish.
When you first open Skipfish, a Terminal window will pop up showcasing the Skipfish commands.

Skipfish can use built-in or customizable dictionaries for vulnerability assessment.

Kali Linux: Vega tool

Vega is a security testing tool used to crawl a website and analyze page content to find links as well as form parameters.

To launch Vega, go to Web Applications | Web Vulnerability Scanners and select Vega.

Vega will flash an introduction banner and display a GUI.

Thank You