EC-Council

The Ethical Hacker's Guide To Hacking Webservers

HACKING WEBSERVERS

1. Information Gathering

The attacker collects as much information as possible and analyzes it to find lapses in the current security mechanism of the webserver.

2. Web Server Footprinting

The purpose of footprinting is to learn about the security aspects of a web server with the help of tools or footprinting techniques.

3. Website Mirroring

In this method, the attacker copies a website and its content onto another server for offline browsing.

4. Vulnerability Scanning

The attacker uses specific tools like Wireshark and Metasploit, to find vulnerabilities and misconfigurations in a web server.

5. Session Hijacking

The attacker takes over complete control of the user's session using session hijacking techniques, like session fixation or session side jacking.

6. Webserver Password Hacking

Attackers use password cracking methods such as brute force attacks, hybrid attacks, and dictionary attacks to crack a webserver's password.

WEBSERVER OPERATIONS - COMPONENTS

1. DocumentRoot

It is one of the web server's root file directories that stores critical HTML files related to the web pages of a domain name that will serve in response to the requests.

2. Server Root

It is the top-level root directory under the directory tree in which the server's configuration and error, executable and log files are stored.

3. Virtual Document Tree

It provides storage on a different machine or a disk after the original disk is filled-up. It is case sensitive and can be used to provide object-level security

4. Virtual Hosting

It is a technique of hosting multiple domains or websites on the same – server. This allows sharing of resources between various servers.

5. Web Proxy

A proxy sever sits in between the web client and web server. Due to the placement of web proxies, all the requests, from the clients will be passed on to the webserver through the web proxies.

Open Source Web ServerArchitecture

OpenSource Web server architecture typically uses **Linux, Apache, MYSQL, and PHP (LAMP)** as principal documents.

Linux is the server's OS that provides secure platform for the webserver

Apache is the web server component handles each HTTP request and response

MySQL is a relational database used to store the web server's content and configuration information

PHP is the application layer technology used to generate dynamic web content.

Web Server Security Issue

Attackers usually target **software vulnerabilities** and configuration errors to compromise web servers.

Network and **OS level** attacks can be well defended using proper network security measures

Such as firewalls, IDS, etc. However, web servers are accessible from anywhere on the web, which makes them **more vulnerable** to attacks.

Stack 1 – Security – IPS/IDS

Stack 2 – Network - Router/Switch

Stack 3 – Operating System - Windows /Linux/OSX

Stack 4 – Database – Oracle/ MYSQL /MSSQL

Stack 5 – Webserver – Apache /Microsoft IIS

Stack 6 – Third party components – OpenSource / Commercial

Stack 7 – Custom web applications – Business logic flaws

Common goals behind a web server attack

Stealing credit cards, or other credentials using phishing techniques.

Hiding and redirecting traffic

Escalating privileges

Compromising a database

Web Server attacks go beyond financial gains, many personal

Attributions leading to the attack:

Curiosity

Achieving self-set challenge

Damage target organizations reputation.

1.Why web servers are compromised?

Improper file and directory permissions

Installing servers with default settings

Unnecessary services enabled, including content management and remote administration

Security conflicts with business ease-of-use case

Lack of proper security policy, procedures, and maintenance

Improper Authentication with external systems

CONT

Default accounts with their default passwords, or no passwords

Unnecessary default, backup or sample files

Misconfigurations in web server, OS, and networks

Bugs in server software OS, and web applications

Misconfigured SSL certificates and encryption settings

Administrative or debugging functions that are enabled or accessible on web servers

Use of self-signed certificates and default certificates.

Impact of web serverAttacks

User account compromised

Website defacement

Secondary attacks from the website

Root access to other applications and servers

Data tampering and data theft

Web Server Attacks

DoS,DDoS Attack–

Attackers may send numerous fake requests to the webserver which results in the web server crashing or becoming unavailable to the legitimate users

Attackers may target high profile web servers such as banks, credit card payments gateways, government owned services etc. to **steal user credentials.**

To crash the web server running the application, attacker targets the following services by consuming the web server with fake requests.

· Network bandwidth

· Server memory

· Application exception handling mechanism

· CPU Usage

· Hard disk space

· Database space.

DNS Server Hijacking

Attacker compromises DNS server and changes the DNS settings so that all the requests, coming towards the target web server are redirected to his/her own malicious server.

Domain Name System (DNS) resolves a domain name to its corresponding IP address. In DNS hijacking, an attacker compromises the DNS server and changes the mapping settings of the target DNS server to redirect toward a rogue DNS server so that it would redirect the user's request to the attacker's rogue server. Thus, when the user type the legitimate URL in a browser, the settings will redirect to the attackers fake site.

DNS Amplification Attack

Attacker takes advantage of **DNS recursive method** of DNS redirection to perform DNS amplification attack.

Attacker uses compromised PCs with **spoofed IP addresses** to amplify the DDOS attacks on victim's DNS server by exploiting DNS recursive method.

Directory Traversal Attack

The attacker uses ../(dot-dot-slash) sequence to access restricted directories outside of the web server root directory

Attacker scan use **trial and error method** to navigate outside of the root directory and access sensitive information in the system.