**Module 13: Hacking Web Servers**

**Web Server Operations**

* **Components:**
  + **Document Root:** Store critial HTML files related to the web pages of a domain name that will be served in response to the requests.
  + **Server Root:** Store server’s configuration, error, executable, and logs
  + **Virtual Document Tree:** Provide storage on a different machine or disk after the original disk if filled up
  + **Virtual Hosting:** Technique of hosting multiple domains or websites on the same server
  + **Web Proxy:** Sit between the web client and web server to prevent IP blocking and maintain anoymity
* **Issues**
  + Attack targets **software vulnerabilities** and configuratrion errors
  + **Network** and **OS level** attacks can be well defended using proper network security measures such as firewalls, IDS, etc. Web server can be accessed from anywhere via the Internet, which renders them highly vulnerable to attacks
* **Why are Web Servers Compromised?**
  + Improper file and dir permissions
  + Installation with default settings
  + Enabling of unnecessary services
  + Security conflicts with businese ease-of-use case
  + Lack of proper security policies, procedures, and maintenance
  + Improper authentication with external systems
  + Default accoutns having default passwords, or no passwords
  + Unnecessary default, backup, or sample files
  + Misconfiguration 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 enbaled or accessible on web servers
  + Use of self-signed certificates and default certificates

**Web Server Attacks**

**Web Server Attacks**

* **DoS/DDoS Attacks**
* **DNS Server Hijacking**
* **DNS Amplification Attack:** Take the adv of the **DNS recursive method** of DNS redirection to perform DNS amplification attacks. Attacks use compromised PCs with **spoofed IP address** to…
* **Directory Traversal Attacks:** Attackers use the **../** seq to access restricted dir outside the web server root dir.
* **MITM/Sniffing Attack**
* **Phishing Attacks**
* **Website Defacement**
* **Web Server Misconfiguration**
* **HTTP Response-Splitting Attack:** Involve adding header response data into the input field so that the server splits the ressponse into two responses. The attacker can control the first response to redirect the user to a malicious website wheras the other responses are discarded by the web browser
* **Web Cache Poisoning Attack:** Attackers **swap cached content** for a random URL with infected content
* **SSH Brute Force Attack:** SSH tunnels can be used to transmit malwars and other exploits to victims without being detected
* **Web Server Password Cracking:** Mainly target SMTP server, Web Shares, SSH Tunnels, Web form authentication cracking, FTP servers.
* **SSRF (Server-side Request Forgbery) Attack:** Attackers **send crafted requests** to the internal or back end servers by exploiting SSRF vulnerabilities in a public web server.

**Web Application Attacks**

* Parameter/Form Tampering
* Session Hijacking
* DoS Attack
* CSRF
* Cookie Tampering
* SQL injection
* XSS
* Command Injection Attacks
* Unvalidated Input and File injection Attacks
* Directory Traversal
* Buffer Overflow Attacks
* Source Code Disclosure

**Web Server Attack Methodology**

* **Info gathering:** 
  + Search the **Internet, newsgroups, bulletin boards**…
  + Use tools such as **Whois.net** and **Whois Lookup**.
  + Gather info from **Robots.txt** file, it lists **web server dirs and files** that the web site owner wants to hide from web crawlers.
* **Web Server Footprinting/Banner Grabbing:**
  + Gather **valuable system-level data** such as account detailsm OS, software versions, server names, and database schema details
  + **Telnet** a web server to footprint a web server and gather info such as server name, server type, OS, and applications running
  + Use tools such as **Netcraft, httprecon, and ID Serve** to perform footprinting
  + **Netcat:** Read and write data across network connections, using TCP/IP protocol
  + **Telnet:** Probe HTTP servers to determine the Server field in the HTTP response header
  + **NMAP:** **Enumerate web server info** by using commands and **NSE scripts**.
* **Website Mirroring**
  + Create a complete profile of the site’s **dir structure, file structure, external links**, etc
  + Use tools such as **NCollector Studio**, **HTTrack Web Site Copier**, **WebCopier Pro**, etc.
  + Finding Default Credentials of Web Server **(Independent)**
  + Finding Default Content of Web Server **(Independent)**
  + Finding Directory Listings of Web Server **(Independent)**
* **Vulnerability Scanning**
  + Tools such as **Acunetix Web Vulnerabilitiy Scanner**, **Fortify WebInspect**
* **Session Hijacking**
  + Techniques such as **session fixation, session sidejacking, XSS**, etc.
  + Tools such as **Burp Suite, JHijack, Ettercap**
* **Web Server Passwords Hacking**
  + Tools such as **Hashcat, THC Hydra, Ncrack**
* **Using Application Server as a Proxy (Independent)**
  + Attackers use **GET** and **CONNECT** requests to use vulnerable web servers as proxies to connect…

**Web Server Attack Tools**

* **Metasploit**
  + **Exploit Module**: Basic module in Metasploit used to e**ncapsulate an exploit**
  + **Payload Module:** Establish **a communication channel** between the MSF and the target. Combine the arbitary code that is executed because of the success of an exploit.
  + **Auxiliary Module:** Can be used to perform arbitrary, one-off actions such as port scanning, DoS, and even fuzzing.
  + **NOPS Module:** Generate a no-operation instruction used for blocking out buffers. Use **generate** command to generate a NOP sled of arbitrary size and display it in a specific format.
* **Immunity’s CANVAS**

**Countermeasures**

* Place web servers in separate secure server security segment on Network
* Patches and updates
* Protocols and Accounts
* Files and Dirs

**Detect Web Server Hacking Attempts**

* A website change detection system
* Ports, Server Certificates, Machine.config, Code Access Security

**Defend against HTTP RespONSE-Splitting and Web Cache Poisoning**

* **Server Admin**
* **Application Developers:** Comply with **RFC 2616** specifications for **HTTP/1.1**
* **Proxy Server:** Avoid sharing **incoming TCP connections** among different clients. Use different TCP connections with the proxy for different **virtuals hosts**. Implement “maintain request host header” corrently.

**Defend Against DNS Hijacking**

* Choose a registrar accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) and encourage them to set REGISTRAR-LOCK on the domain name.
* Safeguard the registrant’s account information.
* Include DNS hijacking in incident response and business continuity planning.
* Use DNS monitoring tools/services to monitor the IP address of the DNS server and set up alerts.
* Avoid downloading audio and video codecs and other downloaders from untrusted websites.
* Install an antivirus program and update it regularly.
* Change the default router password.
* Restrict zone transfers and use script blockers in the browser.
* **Domain Name System Security Extensions (DNSSEC):** It adds an extra layer to DNS that prevents it from being hacked.
* **Strong Password Policies and User Management:** The use of strong passwords further enhances security.
* **Better Service Level Agreements (SLAs) from DNS Service Providers:** When signing up for DNS servers with DNS service providers, learn who to contact when an issue occurs, how to receive good-quality reception and support, and whether the DNS server’s infrastructure is hardened against attacks.
* **Configuring a Master-Slave DNS within your Network:** Use a master-slave DNS and configure the master without Internet access. Maintain two slave servers so that even if an attacker hacks a slave, it will update only when it receives an update from the master.
* **Constant Monitoring of DNS Servers:** The constant monitoring of DNS servers ensures that a domain name returns the correct IP address.
* **Ensure Router Safety:** Change the default username and password of the router. Keep the firmware up to date for ensuring safety from new vulnerabilities.
* **Use VPN Service:** Establish virtual private network (VPN)-encrypted tunnels for secure private communication over the Internet. This feature protects messages from eavesdropping and unauthorized access.

**Patches and Hotfixes**

* **Hotfix:** An update fo fix a specific customer issue
* **Patch:** Small piece of software designed to fix problems
* **Patch Management:** A process used to fix known vulnerabilities by ensuring the appropriate patches are installed.
* **Patch Management Process**
  + **Detect**
  + **Assess**
  + **Acquire**
  + **Test**
  + **Deploy**
  + **Maintain**
* Patch Management Tools: **GFI LanGuard**

**Web Application Security Scanners**

* Syhunt Hybrid
* N-Stalker X
* ScanMyScanner

**Web Server Malware Infection Monitoring Tools**

* QualysGuard Malware Detectoin

**Web Server Security Tools**

* Fortify WebInspect

**Web Server Pentesting Tools**

* CORE Impact
* Immunity CANVAS