Case Study: Web Application Security Audit Using Nmap

1.What is the significance of finding open ports like 80 (HTTP) and 443 (HTTPS) on a web server? What risks do these open ports pose?

HTTP port 80 is used to carry unencrypted web traffic. It is risky because information sent over this port is susceptible to interceptions or changes by unauthorized parties, which can result in man-in-the-middle (MITM) attacks.

HTTPS port 443 is where encrypted web traffic is routed. SSL/TLS protocols and certificates need to be configured carefully to prevent vulnerabilities, even though they are more secure than HTTP. Attacks like SSL stripping and protocol downgrade attacks can target a server due to inadequate configurations or support for antiquated protocols.

Risks: Services that are exposed to the internet through open ports may be exploited by hackers to take over a system or obtain sensitive data if they are running software that is not secure or is incorrectly configured.

2.Why is it important to identify service versions during a security audit? How can outdated versions, such as Apache 2.4.6, pose a risk to the network?

The significance of determining service versions in a security audit lies in the fact that it enables security teams to evaluate whether the program contains known vulnerabilities. Software that is too old, such as Apache 2.4.6, may have security holes that hackers can take advantage of. In this example, the flaw is CVE-2017-7679.

Risk: The network's attack surface may grow as a result of older versions not having the most recent security patches. Unpatched software, for instance, may be open to buffer overflows, privilege escalation, and remote code execution.

3. What are the potential consequences of running web services that support weak ciphers, such as RC4 and 3DES, in an SSL/TLS configuration?

RC4 and 3DES are examples of weak ciphers that are susceptible to a variety of attacks, including BEAST, RC4 biases, and other cryptographic exploits. Attackers may be able to decrypt HTTPS traffic if these ciphers are used, which could reveal private data like banking information or login credentials.

Consequences: The confidentiality and integrity of encrypted communications are compromised when weak ciphers are permitted. Hackers may be able to crack the encryption, which could result in sensitive data being compromised, data leaks, and man-in-the-middle attacks.

4.Explain the risks of allowing outdated protocols like TLSv1.0 on a web server. What are the recommended best practices for SSL/TLS configurations?

There are several known vulnerabilities in the Transport Layer Security protocol's older version, TLSv1.0. Attackers can use this protocol's flaws to launch attacks like BEAST or Padding Oracle attacks, which crack encryption and reveal private information.

Top Techniques:

Turn off TLSv1.0 and TLSv1.1, then set the server up to only support TLSv1.2 or TLSv1.3.

Employ robust encryption methods such as AES256 and guarantee that forward secrecy (through ECDHE, for example) is activated to safeguard the privacy of previous exchanges.

Enforce secure connections by turning on HTTP Strict Transport Security (HSTS).

5.How does Nmap's SSL scanning script help in assessing the security of HTTPS services? What specific issues did it identify in this case?

Nmap's SSL scanning script assists in evaluating the security of HTTPS services by looking through the SSL/TLS certificate details of the server, including its validity period, issuing authority, supported cipher suites, and potential vulnerabilities related to out-of-date protocols or weak encryption algorithms. This helps identify problems such as expired certificates, insecure cipher suites, or the use of weak hashing algorithms, which could jeopardize the security of the HTTPS connection.

In this case, the script showed that the server was using out-of-date protocols (TLSv1.0) and weak ciphers (RC4, 3DES). Additionally, it highlighted the lack of forward secrecy, which is essential to stopping significant breaches from decrypting previous sessions.

6.What is the purpose of using Nmap's `--script vuln` command, and how did it help detect vulnerabilities like CVE-2017-7679 and CVE-2015-3418?

Nmap's --script vuln command runs particular scripts to search for known vulnerabilities in services, automating the vulnerability scanning process.

In this case, the script found:

A buffer overflow in Apache HTTPD that might enable remote code execution is known as CVE-2017-7679.

PHP vulnerability CVE-2015-3418: This one might let hackers get around security measures.

The security team uses these findings to help identify high-priority vulnerabilities that require quick fixes.

7.Why is enabling HTTP Strict Transport Security (HSTS) important for web applications? What potential attacks does it mitigate?

HSTS ensures that browsers always use **HTTPS** to access the website, preventing users from accidentally connecting over HTTP. It also helps mitigate **SSL stripping** attacks, where an attacker downgrades a secure HTTPS connection to HTTP, exposing sensitive data.

Mitigated Attacks: SSL stripping, man-in-the-middle attacks, and protocol downgrade attacks.

8.What is the risk associated with an outdated PHP version (like 5.4.16)? What steps should be taken to mitigate this risk?

PHP versions that are outdated frequently have known vulnerabilities. In this case, arbitrary file uploads, privilege escalation, and remote code execution (RCE) are among the several vulnerabilities that affect PHP 5.4.16.

Mitigation: Install security patches on a regular basis and upgrade to a supported and secure version of PHP (such as 7.4 or later). Examine PHP configurations to make sure best security practices—disabling superfluous modules, for example—are followed.

9. How can the MySQL authentication bypass vulnerability (CVE-2012-2122) be exploited, and what measures should be taken to secure the database?

A MySQL authentication bypass vulnerability called CVE-2012-2122 lets attackers obtain access by continuously attempting to authenticate. Sometimes, without knowing the actual credentials, attackers can bypass authentication due to a flaw in the password comparison function.

Steps to Protect the Database:

Install a patched version of MySQL to address the vulnerability.

Put firewall rules in place to limit database access to trusted IP addresses only.

Make sure robust authentication measures are implemented, and when connecting to databases, use encryption.

10.What are some ways to prevent unauthorized access to internal services exposed on unexpected ports like 8080?

Unexpected open ports, such as 8080, may expose internal systems to outside attacks, which could result in illegal access or possibly the exploitation of inadequately secured APIs.

Preventive actions: Close unused ports or limit access by limiting access to trusted IP addresses only using firewall rules. To guarantee that only authorized users can connect to services on these ports, implement access controls.Make sure the network is regularly scanned to make sure that only necessary ports are open, and think about segmenting the network to isolate important services.