CYB 552 – WEB APP NMAP

1.) Ports 80 and 443 are essential for online traffic. Port 80 is used for unsecured HTTP connections, whereas port 443 is reserved for secure HTTPS connections. Their existence shows that the server is configured to efficiently manage web traffic. Risks: attackers used open ports as a point of entry. Particularly susceptible to assaults such as man-in-the-middle (MITM), which can result in data interception, is port 80. Furthermore, if HTTPS is misconfigured or not enforced, sensitive data is exposed via HTTP. Open ports further expand the attack surface, as they can be targeted by exploitation tools and scanners.

2.) Determining service versions in a security audit is essential to comprehending the possible weaknesses linked to software. Different versions of software include known flaws that can be exploited. Dangers of Outdated Versions: For example, Apache 2.4.6 has several security vulnerabilities. Running out-of-date versions can put the network at risk for denial of service (DoS) attacks, buffer overflow assaults, and remote code execution, among other threats. Attackers frequently use these known vulnerabilities to penetrate systems, making quick fixes critical.

3.) Weak ciphers like RC4 and 3DES are easily cracked by contemporary computing techniques, supporting them carries significant risks. They made it possible for hackers to decode traffic, it results in data tampering or theft. Furthermore, if a secure connection is breached, attackers attempt session hijacking or exploit sensitive information transmitted between clients and servers.

4.) TLSv1.0 is regarded as antiquated and vulnerable to a few attacks, such as BEAST and POODLE. Older protocols may include encryption flaws that let hackers intercept or alter data while it's in transit.  
recommended Best Practices:   
  
 a.) TLS 1.2 or later is the most recent version that should be used.   
 b.) Make the SSL/TLS setup up to date and that the supported ciphers and protocols are being used.   
 c.) To guarantee that clients always utilize HTTPS, use HSTS.

5.) Security Assessment: Nmap's SSL scanning script examines SSL/TLS service settings for supported ciphers and protocol versions. In this scenario, the scan identified the usage of weak ciphers such as RC4 and 3DES, as well as the lack of forward secrecy, suggesting that the server's SSL/TLS implementation was insufficient to protect against current attacks.

6.) To check for known vulnerabilities in services that are operating on a target, use the --script vuln command. It uses a database of Common Vulnerabilities and Exposures (CVEs) to find vulnerabilities unique to the software versions discovered.   
Detection of Vulnerabilities: In this scenario, it effectively identified vulnerabilities such as CVE-2017-7679 (buffer overflow in Apache) and CVE-2015-3418 (PHP security bypass), revealing major flaws that attackers exploit.

7.) Alerting browsers to only connect to the server via HTTPS, HSTS lowers the danger of downgrade and Man-in-the-Middle (MITM) attacks. It ensures that even if a user makes an HTTP request, the browser converts it to HTTPS, hence requiring secure communications.  
  
8.) Risks: An out-of-date PHP version, such as 5.4.16, is susceptible to a variety of vulnerabilities, including remote code execution and code injection problems. These can result in illegal data access, modification, or control of the system. Steps for Mitigation: It's important to upgrade to a secure, supported version of PHP, such 7.4 or later. Additionally, completing frequent code reviews, applying security best practices, and implementing input sanitization can all assist to mitigate vulnerabilities.  
  
9.) Exploitation: With escaping authentication checks, attackers get unauthorized access to the MySQL database, potentially resulting in data loss or theft.  
Security Measures: To reduce this risk, it is critical to patch the MySQL server to eliminate vulnerability. Additionally, adopting stringent access rules, segmenting the database network, and using IP whitelisting helps improve database security.

10.) Methods of Prevention:

a.) Setting strong firewall rules into place to limit access to only reputable and well-known IP addresses.   
 b.) Turning off unused ports (such as 8080) unless they are necessary for a particular function.   
c.) Accessing internal services with VPNs reduces exposure to the public internet.   
identifying and fixing any possible vulnerabilities pertaining to internal services through routine penetration tests and security audits.   
d.) Use application-layer firewalls to filter and monitor traffic to internal services for harmful activities.