Task2: Vulnerability scan reports, analysis of high-risk vulnerabilities

Port	Service	Vulnerability	Description	CVSS Score	Recommended Solution
22	SSH	Brute Force Login with Default Credentials	Default credentials allow remote attackers to access the server via SSH.	9.8	Change SSH default credentials immediately.
21	FTP	Brute Force Login	Weak credentials allow unauthorized access to the FTP server.	7.5	Update passwords to stronger ones as soon as possible.
80	HTTP	XSS and Command Execution (CVE-2008-5304, CVE-2008-5305)	Cross-site scripting and command injection vulnerabilities, leading to unauthorized script/code execution.	10	Use HTTPS Protocol Port 443
1099	Java RMI	Insecure Default Configuration (CVE-2011-3556)	Incorrect configuration of Java RMI allows remote code execution by unauthenticated attackers.	7.5	Disable class-loading and consult the vendor for additional guidance.
512	relaxed	Unencrypted Login (CVE-1999-0618)	Unencrypted transmission of credentials allowing remote attackers to execute shell commands.	10	Disable rexec and switch to SSH for secure communication.
3306	MySQL	Default Credentials (CVE-2001-0645)	Remote attackers can log in as root with an empty password, posing a high risk of unauthorized database access.	9.8	Change the MySQL root password immediately.

5432	PostgreSQL	Default Credentials (PostgreSQL Protocol)	Weak credentials allow remote login to PostgreSQL as user "postgres."	9	Secure PostgreSQL with strong passwords.
5900	VNC	Brute Force Login	Weak or default password allows unauthorized remote access via VNC.	9	Set a strong, complex VNC password.
8009	Apache JServ	Ghostcat RCE (CVE-2020-1938)	Remote code execution vulnerability in Apache Tomcat's AJP connector allowing attackers to access webapp files.	9.8	Upgrade Apache Tomcat to a patched version (7.0.100, 8.5.51, 9.0.31).
6200	vsftpd	Backdoor Vulnerability (CVE-2011-2523)	Compromised source packages allow attackers to open a shell on port 6200.	9.8	Download and install the patched version of vsftpd.
3632	DistCC	Remote Code Execution (CVE-2004-2687)	DistCC allows malicious clients to execute arbitrary commands due to a misconfigured server.	9.3	Apply vendor patches and restrict access.
8787	dRuby/DRb	Remote Code Execution (RCE)	Distributed Ruby (dRuby/DRb) allows remote code execution through improper authorization and $SAFE level configuration.	10	Set $SAFE to appropriate levels and implement proper access control.
514	rsh	Unencrypted Cleartext Login (CVE-1999-0651)	Remote shell (rsh) service allows execution of shell commands without	7.5	Disable rsh and use SSH for secure communications.

			encryption or password.		

Used Tools: OpenVAS

Delivered by: **Eslam Ahmed**