Vulnerability scanning assessment, multiple critical and high-severity vulnerabilities were identified on the target host 192.168.0.102. The most severe findings include an exposed vsftpd 2.3.4 backdoor, an open bind shell on port 1524 providing root access, and an outdated Apache HTTP Server (2.2.8). These issues allow attackers to gain unauthorized access and potentially fully compromise the system. Additional high-risk findings include insecure services such as Telnet, RSH/Rlogin, exposed SMB, Java RMI, and outdated database services (MySQL and PostgreSQL), all of which significantly increase the attack surface.

Title: Critical FTP Vulnerability
Findings: vsftpd 2.3.4 backdoor vulnerability identified on **Host: 192.168.0.102**, allowing remote attackers to gain unauthorized root access. **CVSS Score: 10.0**
Remediation: Remove or upgrade the FTP service to a secure version and disable FTP if not required.

Title: Insecure Remote Access Service
Findings: Telnet service enabled on **Host: 192.168.0.102**, transmitting credentials in clear text and exposing the system to interception attacks. **CVSS Score: 8.5**
Remediation: Disable Telnet and replace it with secure protocols such as SSH.

Title: Critical Bind Shell Exposure
Findings: An open bind shell on **Port 1524** was discovered on **Host: 192.168.0.102**, providing direct root-level access. **CVSS Score: 10.0**
Remediation: Immediately close the bind shell port and investigate the system for compromise.

Title: Critical Web Vulnerability
Findings: Outdated Apache HTTP Server version 2.2.8 detected on **Host: 192.168.0.102**, exposing the server to known remote exploitation risks. **CVSS Score: 9.0**
Remediation: Patch and upgrade Apache HTTP Server to the latest stable version.

Title: Exposed SMB Services
Findings: SMB services running on **Ports 139 and 445** were identified on **Host: 192.168.0.102**, increasing the risk of unauthorized access and lateral movement. **CVSS Score: 8.0**
Remediation: Restrict or disable SMB services and enforce proper access controls.

Title: Insecure Legacy Services
Findings: RSH and Rlogin services enabled on **Ports 512 and 513** on **Host: 192.168.0.102**, allowing insecure remote command execution. **CVSS Score: 8.8**
Remediation: Disable RSH and Rlogin services and use secure remote management methods.

Title: Outdated Database Service (MySQL)
Findings: MySQL version 5.0.51a detected on **Host: 192.168.0.102**, containing multiple known vulnerabilities. **CVSS Score: 7.5**
Remediation: Upgrade MySQL to a supported and patched version and restrict database access.

Title: Outdated Database Service (PostgreSQL)
Findings: PostgreSQL version 8.3.x identified on **Host: 192.168.0.102**, which is end-of-life and vulnerable to exploitation. **CVSS Score: 7.4**
Remediation: Upgrade PostgreSQL to a secure, supported release.

Title: Exposed Remote Desktop Service
Findings: VNC service exposed on **Port 5900** on **Host: 192.168.0.102**, potentially allowing unauthorized remote desktop access. **CVSS Score: 6.5**
Remediation: Disable VNC if not required or restrict access using strong authentication and firewall rules.

Title: Java RMI Exposure
Findings: Java RMI Registry service exposed on **Port 1099** on **Host: 192.168.0.102**, increasing the risk of remote code execution. **CVSS Score: 7.5**
Remediation: Restrict or disable Java RMI services and apply security updates.

Title: Exposed Application Server
Findings: Apache Tomcat service exposed on **Port 8180** on **Host: 192.168.0.102**, potentially vulnerable to application-layer attacks. **CVSS Score: 7.0**
Remediation: Restrict access to Tomcat services and apply the latest patches.

Title: RPCBind Service Exposure
Findings: RPCBind service exposed on **Port 111** on **Host: 192.168.0.102**, which may assist attackers in service enumeration. **CVSS Score: 6.0**
Remediation: Disable RPCBind if not required or restrict access via firewall rules.

Subject : Critical Vulnerabilities Identified on 192.168.0.102 – Immediate Action Required

Hi Team,

During a vulnerability assessment on host **192.168.0.102**, multiple **critical and high-severity vulnerabilities** were identified. Notably, an exposed **vsftpd 2.3.4 backdoor (CVSS 10.0)** and an **open bind shell on port 1524** allow direct root-level access.
PoC: Using Nmap service enumeration, these services were confirmed reachable externally, and known public exploits exist that enable remote compromise without authentication.

Immediate remediation is required, including disabling insecure services, closing unused ports, and upgrading outdated software such as Apache, databases, and remote access services.

Please prioritize fixes and confirm once remediation is complete.

Regards,
Shashank M.