5. ISC BIND 9.4.2 (DoS/Cache Poisoning Vulnerabilities)

- **Finding:** Outdated DNS server vulnerable to DoS and cache poisoning attacks.
- **Remediation:** Upgrade to a **supported BIND version**. Apply DNSSEC and restrict zone transfers.

6. Apache httpd 2.2.8 (Multiple Vulnerabilities, CVE-2007-6750, CVE-2011-3192)

- **Finding:** Old Apache version with vulnerabilities that allow DoS and remote exploits.
- **Remediation:** Upgrade Apache to the latest version. Apply security patches. Disable unnecessary modules.

7. RPC Services Exposed (rpcbind, nfs)

- **Finding:** Exposed RPC services allow attackers to gather system info and exploit NFS.
- **Remediation:** Disable unused RPC services. Restrict NFS access to trusted hosts.

8. Samba 3.x–4.x (Remote Code Execution, CVE-2007-2447)

- **Finding:** Samba vulnerable to remote code execution due to unsafe handling of inputs.
- **Remediation:** Patch Samba to the latest version. Restrict SMB shares to authenticated users.

9. rlogin Service Enabled (Cleartext Auth)

- **Finding:** rlogin transmits credentials without encryption.
- **Remediation:** Disable rlogin. Replace with SSH.

10. Netkit-rsh rexecd (Insecure Remote Execution)

- **Finding:** Allows unauthenticated or weakly authenticated remote command execution.
- **Remediation:** Disable rexecd service. Use SSH with strong authentication.

11. Netkit rshd (Remote Shell, Cleartext)

- **Finding:** rshd provides shell access without encryption.
- **Remediation:** Disable rshd. Replace with SSH.

12. Metasploitable Root Shell Service

- **Finding:** Service provides direct root shell, trivial full compromise.
- **Remediation:** Disable/remove root shell service. Use only secure admin access with strong authentication.

13. NFS (Unauthenticated Share Access)

- **Finding:** NFS exports allow unauthenticated access, exposing files to attackers.
- **Remediation:** Restrict NFS shares to specific IPs. Use authentication (Kerberos).

14. ProFTPD 1.3.1 (Backdoor in Some Builds)

- **Finding:** Vulnerable builds include a backdoor allowing remote access.
- **Remediation:** Upgrade ProFTPD to the latest secure version. Disable FTP if not required.

15. MySQL 5.0.51a (Weak Auth, Known Vulnerabilities)

- **Finding:** MySQL service is outdated and may allow weak authentication or SQL injection.
- **Remediation:** Upgrade to a supported MySQL/MariaDB version. Enforce strong passwords and patch vulnerabilities.

16. PostgreSQL 8.3.x (Weak Auth, CVEs)

- **Finding:** Old PostgreSQL version vulnerable to privilege escalation and DoS.
- **Remediation:** Upgrade PostgreSQL to the latest supported release. Restrict remote access.

17. VNC (No Encryption, Default Password Risk)

- **Finding:** VNC transmits credentials without encryption, and often uses default passwords.
- **Remediation:** Disable VNC or tunnel over SSH. Use VNC with strong authentication and encryption.

18. X11 Service Open (Unauthenticated Access)

- **Finding:** Open X11 allows attackers to capture keystrokes/screens remotely.
- **Remediation:** Disable X11 remote access or restrict to localhost. Use SSH tunneling for X forwarding.

19. UnrealIRCd (Backdoor, CVE-2010-2075)

- **Finding:** Backdoored version allows remote attackers to execute arbitrary commands.
- **Remediation:** Remove or upgrade UnrealIRCd to a verified clean version.

20. Apache Jserv Protocol (AJP13) Exposed

- **Finding:** AJP connector exposed, may allow remote file inclusion or deserialization attacks.
- **Remediation:** Restrict AJP access to localhost. Apply security patches.

21. Apache Tomcat (5.5/6.0, Manager RCE Vulns)