**Week 1: Compliance & Risk Assessment Report**

**Capstone Project 12 – Cybersecurity Governance & Compliance Frameworks**  
Target Environment: Nigerian Government Healthcare Agency (Simulated via Metasploitable 2)

**1. Introduction**

**Purpose of the Risk Assessment**

This assessment evaluates the cybersecurity risks of a simulated Nigerian government healthcare agency system using Metasploitable 2 as the target. It identifies vulnerabilities, measures their severity, and maps compliance requirements to NDPR (2019), NIST CSF, ISO 27001:2022, and GDPR.

**Scope and Objectives**

* Identify regulatory compliance obligations for the healthcare sector in Nigeria.
* Conduct vulnerability scanning and enumeration of key assets.
* Quantify risks using CVSS, Likelihood, and Impact scores.
* Map findings to compliance controls and recommend governance strategies.

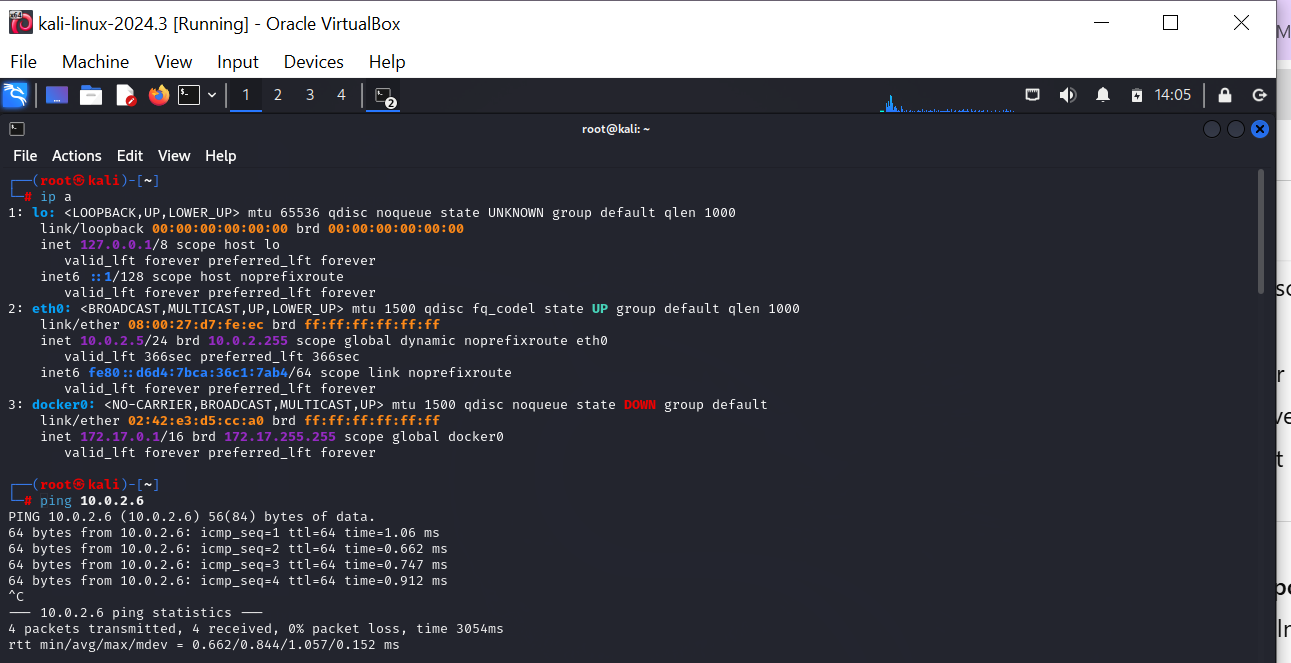
**2. Risk Identification**

**2.1 Key Assets and Systems Identified**

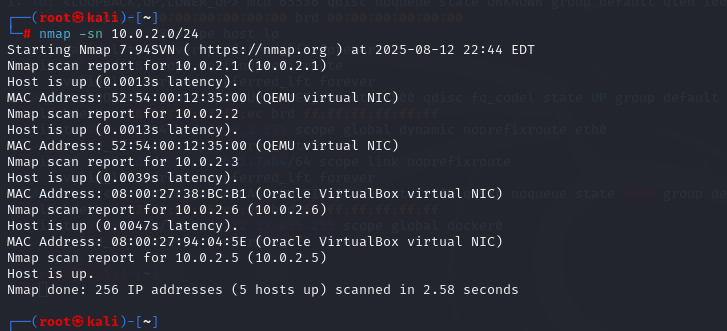
* **Metasploitable 2 Server** at 10.0.2.6 running Linux 2.6 kernel
* Services: FTP, SSH, Telnet, SMTP, DNS, HTTP, SMB, NFS, MySQL, PostgreSQL, Apache Tomcat, VNC, IRC
* Web applications: phpMyAdmin, TikiWiki CMS, Apache test pages, phpinfo.php

**2.2 Scanning Methodology & Screenshot Placeholders**

1. **Host Discovery** – Identify live hosts (Confirm communication with target system)  
   Command:ping 10.0.2.6



1. nmap -sn 10.0.2.6/24 - Discover the Host



1. **Service Enumeration** – Detect open ports and versions

nmap -sV -p- 10.0.2.6 -oN service\_scan.txt

A screenshot of a computer

AI-generated content may be incorrect.

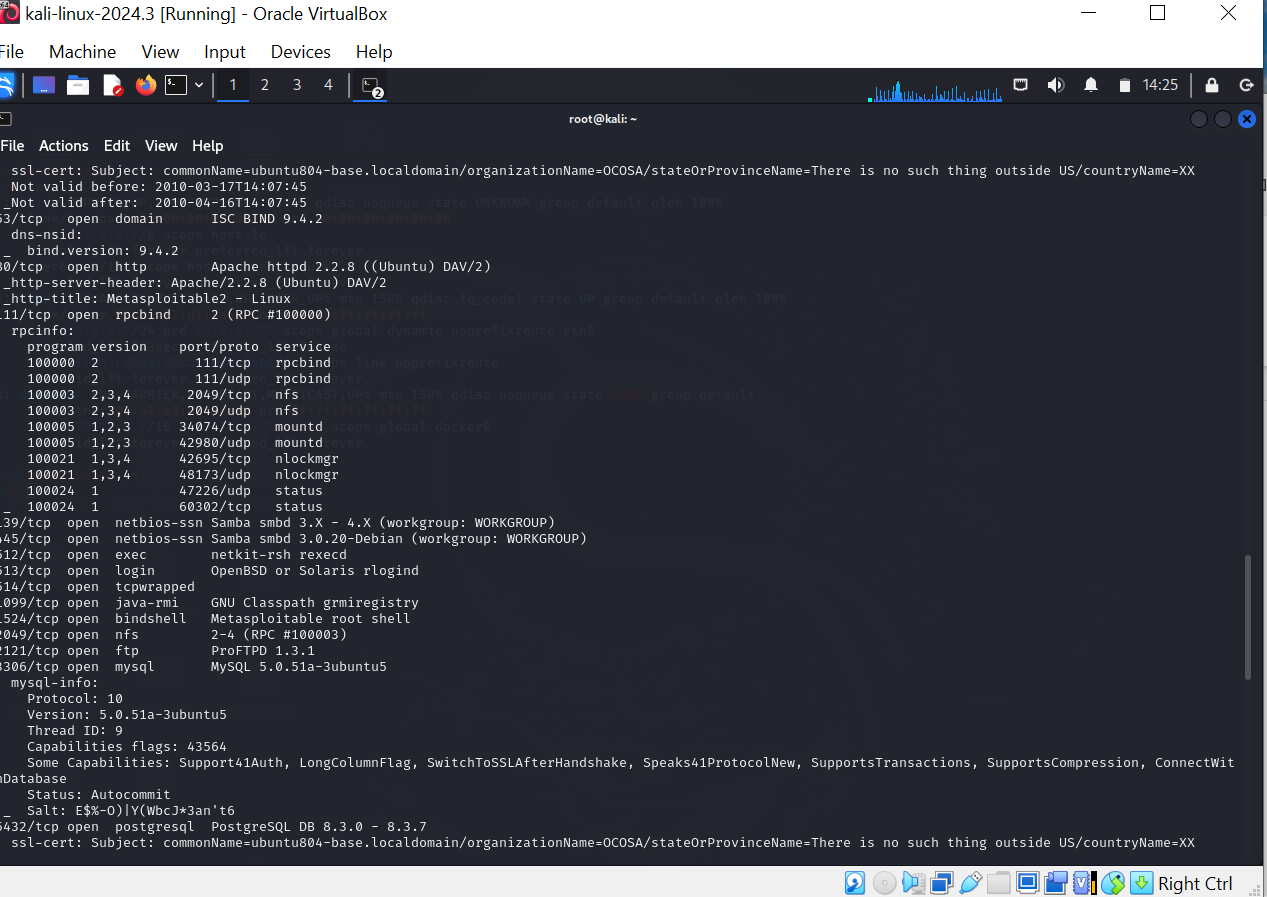
1. **OS & Service Detection** – Deep detection

nmap -A 10.0.2.6 -oN os\_detect.txt

A screenshot of a computer

AI-generated content may be incorrect.

Continuation of nmap -A 10.0.2.6 -oN os\_detect.txt



Continuation of nmap -A 10.0.2.6 -oN os\_detect.txt

A screenshot of a computer

AI-generated content may be incorrect.

Continuation of nmap -A 10.0.2.6 -oN os\_detect.txt

A screenshot of a computer

AI-generated content may be incorrect.

1. **SMB Vulnerability Scan**

nmap -p 139,445 --script smb-vuln\* 10.0.2.6 -oN smb\_vuln.txt

A computer screen shot of a black background

AI-generated content may be incorrect.

1. **FTP Vulnerability Scan**

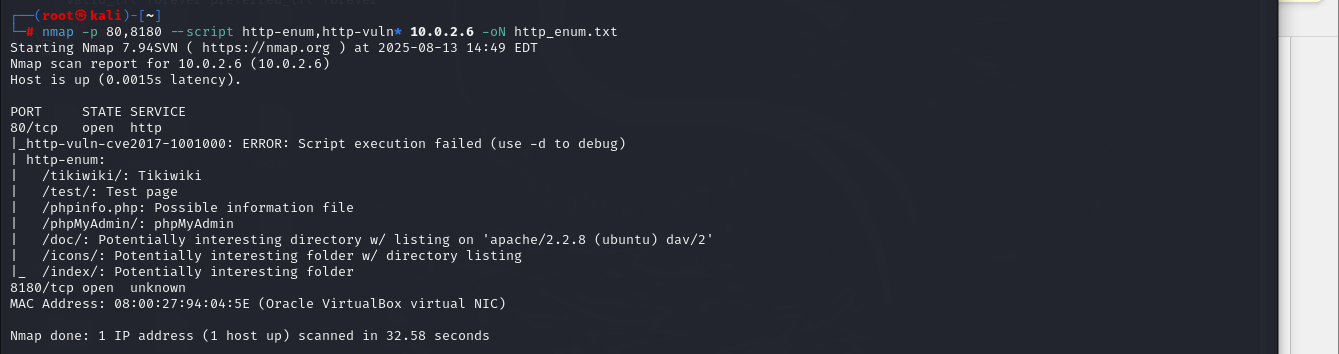
nmap -p 21 --script ftp-anon,ftp-vuln\* 10.0.2.6 -oN ftp\_vuln.txt

A screen shot of a computer

AI-generated content may be incorrect.

1. **HTTP Enumeration & Vulnerability Detection**

nmap -p 80,8180 --script http-enum,http-vuln\* 10.0.2.6 -oN http\_enum.txt



1. **MySQL Vulnerability Scan**

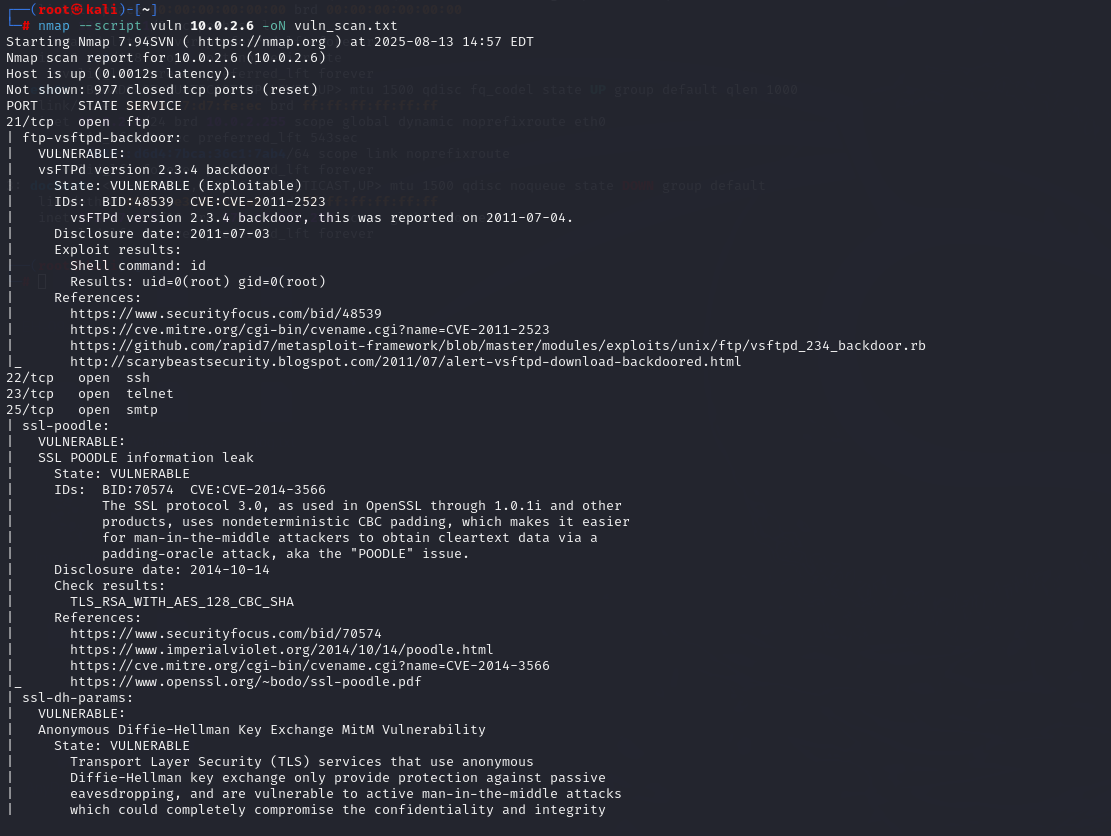
nmap -p 3306 --script mysql-info,mysql-vuln\* 10.0.2.6

A screenshot of a computer

AI-generated content may be incorrect.

1. **Full Vulnerability Scan**

nmap --script vuln 10.0.2.6 -oN vuln\_scan.txt



1. **Summary of all the different scans**

nmap -sV -O -sC -A \ -p- \

--script "default,ftp-anon,ftp-vuln\*,http-enum,http-vuln\*,smb-vuln\*,mysql-info,mysql-vuln\*,vuln" \

10.0.2.6 -oN full\_report.txt -oX full\_report.xml

Converts the xml to html



To open in firefox



**2.3 Summary of Key Vulnerabilities Found**

* **vsFTPd 2.3.4 Backdoor** (CVE-2011-2523) – Remote Code Execution
* **Anonymous FTP Login** – Unauthenticated access
* **Samba RCE** (CVE-2007-2447) – Remote Code Execution
* **Apache HTTPD 2.2.8** – Multiple vulnerabilities
* **SSL POODLE** (CVE-2014-3566) – Weak encryption
* **MySQL 5.0.51a** – CVE-2012-2122 (Outdated with Auth bypass), CVE-2011-2523 (exposure in MySQL context)
* **Tomcat 5.5 Legacy RCE** – Multiple legacy exploits
* **Telnet Service Open** – Insecure cleartext channel

**3. Risk Analysis**

| **Vulnerability** | **CVE ID** | **CVSS Score** | **Likelihood (1-5)** | **Impact (1-5)** | **Risk Level (L×I)** | **Risk Category** |
| --- | --- | --- | --- | --- | --- | --- |
| vsFTPd 2.3.4 Backdoor | CVE-2011-2523 | 9.8 (Critical) | 5 | 5 | 25 | Critical |
| Anonymous FTP Login | N/A | 7.5 (High) | 4 | 4 | 16 | Critical |
| Samba RCE | CVE-2007-2447 | 10.0 (Critical) | 5 | 5 | 25 | Critical |
| Apache HTTPD 2.2.8 Vulns | CVE-2007-6750 | 7.5 (High) | 4 | 4 | 16 | Critical |
| SSL POODLE | CVE-2014-3566 | 5.9 (Medium) | 3 | 3 | 9 | Medium |
| MySQL Auth Bypass | CVE-2012-2122 | 6.5 (Medium) | 3 | 4 | 12 | High |
| Tomcat 5.5 RCE | Multiple CVEs | 9.0 (Critical) | 4 | 5 | 20 | Critical |
| Telnet Service | N/A | 8.0 (High) | 4 | 4 | 16 | Critical |

**Risk Scoring Methodology**

* **CVSS Scores** were obtained from [cvedetails.com](https://www.cvedetails.com), providing a baseline severity (0–10).
* **Likelihood (1–5)**: rated based on exploitability and public availability of exploits.
* **Impact (1–5)**: rated based on potential damage to confidentiality, integrity, and availability.
* **Risk Level**: calculated as Likelihood × Impact (range 1–25).
* **Risk Category**:
  + 1–5 = Low
  + 6–10 = Medium
  + 11–15 = High
  + 16–25 = Critical

**4. Risk Mitigation Strategies**

**1. FTP Service (vsFTPd 2.3.4 Backdoor – CVE-2011-2523)**

* Control: If an updated version is unavailable, decommission vsFTPd 2.3.4 and deploy a supported FTP/SFTP service. Disable anonymous FTP access and enforce SFTP (SSH File Transfer Protocol) with strong authentication mechanisms
* Timeline: Immediate (0–1 week).

**2. SSH (OpenSSH 4.7p1 Weaknesses)**

* Control: Upgrade OpenSSH to the latest supported version. Enforce key-based authentication and disable weak ciphers. Restrict SSH access to trusted IPs only.
* Timeline: Short-term (1–2 weeks).

**3. Telnet Service (Insecure, Unencrypted Protocol)**

* Control: Use Telnet only for testing or validation, else use SSH. Train administrators on secure remote access.
* Timeline: Immediate (0–1 week).

**4. SMTP -Simple Mail Transfer Protocol (SSLv2 Support – Deprecated Encryption)**

* Control: Disable SSLv2 support and configure TLS 1.2/1.3. Update Postfix and enforce STARTTLS (Start Transport Layer Security) with strong ciphers.
* Timeline: Short-term (1–2 weeks).

**5. SMB (Samba 3.0.20 – Unpatched, Null Sessions, Weak Config)**

* Control: Upgrade Samba to a supported version. Enforce SMB (Server Message Box) signing. Disable null sessions and restrict access by firewall rules.
* Timeline: Immediate (0–1 week).

**6. MySQL 5.0.51a Vulnerabilities (including CVE-2012-2122 Auth Bypass)**

* Control: Auth Bypass (CVE-2012-2122): Patch or upgrade to the latest secure release. Restrict database exposure to internal hosts only. Enforce strong authentication and principle of least privilege.
* Disable test databases and remove default accounts.
* Enable logging and monitoring of authentication attempts.
* Timeline: Immediate (0–1 week).

**7. PostgreSQL 8.3.x (Outdated, Potential RCE Vulnerabilities)**

* Control: Upgrade PostgreSQL to a currently supported release. Restrict access to internal applications. Regularly apply security patches.
* Timeline: Medium-term (2–4 weeks).

**8. Apache HTTPD 2.2.8 (CVE-2010-1452, CVE-2011-3192, etc.)**

* Control: Upgrade Apache to a supported LTS version. Apply security patches for mod\_ssl and request handling. Disable directory listing and information disclosure (phpinfo.php, /test/, /doc/).
* Timeline: Immediate (0–1 week).

**9. Apache Tomcat (CVE-2009-3548, CVE-2010-2227, CVE-2010-1157, etc.)**

* Control: Upgrade Tomcat to a supported version. Restrict access to the admin console. Remove default/unused applications. Harden configuration against directory traversal and information leakage.
* Timeline: Short-term (1–2 weeks).

**10. DistCCD Service (Unauthenticated Remote Code Execution – CVE-2004-2687)**

* Control: Disable the distccd service unless strictly required. If required, restrict access to trusted IPs only and upgrade to a patched version.
* Timeline: Immediate (0–1 week).

**11. VNC (Weak Authentication)**

* Control: Enforce strong authentication, use encrypted VNC tunnels, or disable if unnecessary.
* Timeline: Short-term (1–2 weeks).

**12. General Controls Across All Systems**

* Apply a regular patch management program.
* Enforce network segmentation (restrict database and RPC services to internal subnets).
* Deploy firewalls/IPS to monitor and block exploitation attempts.
* Establish a vulnerability management cycle with continuous scanning and remediation.

**5. Conclusion**

**Summary of Findings**

This assessment identified **multiple Critical vulnerabilities** (FTP, Samba, MySQL, Apache, Tomcat, Telnet) that could result in **remote code execution** and full system compromise. For a healthcare agency, this risks patient data confidentiality, integrity and availability risk of medical records, and regulatory non-compliance.

**Next Steps & Monitoring**

* 1. **Immediate Remediation Actions**
* Patch critical vulnerabilities (e.g., CVE-2011-2523 in vsFTPd, CVE-2012-2122 in MySQL, Apache/Tomcat exposures).
* Disable insecure and unnecessary services (RSH, Anonymous FTP, SMB with no signing). Telnet can be used only for testing/troubleshooting and validation but not for secure communication. Enable **SMB signing** or upgrade to **SMBv3** (with encryption). (NIST PR.AC-3, PR.DS-2) (ISO27001:2022 Annex A.8.9, Annex A.8.11, Annex A.8.24)
* Enforce strong authentication and access controls (SSH hardening, password policies).(PR.PS-5)
  1. **Compliance Alignment**
* Map remediation tasks to **NDPR, NIST CSF, ISO 27001, GDPR** controls.
* Update security policies and procedures to address identified compliance gaps.
* Train staff on data protection obligations, incident reporting, and secure system use.
  1. **Monitoring & Continuous Improvement**
* Deploy **intrusion detection(Snort) / SIEM tools(Splunk)** to monitor suspicious activity. (NIST DE:CM-1), (ISO27001:2022 A.8.16), (Art 32(1))
* Schedule **regular vulnerability scans** and **penetration tests** (quarterly or after major changes). (ISO27001:2022 A.8.8), (NIST ID:RA-1), (Art 32(1))
* Establish **compliance monitoring dashboards** for reporting to regulators and internal audit. (ISO27001:2022 A.5.36), (NIST GV:MA-1), (Art 5(2))
  1. **Incident Response Preparedness**
* Define clear escalation procedures for vulnerabilities mapped to GDPR Art. 33 (breach notification within 72 hours).
* Run tabletop exercises to test response to healthcare data breaches.
* Maintain updated contacts for Computer Emergency Response Team(CERT), regulators (NDPC in Nigeria), and law enforcement.
  1. **Governance & Oversight**
* Set up a **Cybersecurity Governance Committee** to review compliance status monthly.
* Assign **risk owners** for each critical system/service. (ISO27001:2022 A.5.3)
* Ensure **board-level reporting** of cybersecurity risks and compliance progress. (ISO27001:2022 Clause 5.1)

**6. Compliance Gap Mapping Table (CVE → NDPR, NIST, ISO 27001, GDPR)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | | **Vulnerability** | **CVE ID** | **NDPR 2019** | **NIST CSF** | **ISO 27001:2022** | **GDPR** | | --- | --- | --- | --- | --- | --- | | **vsFTPd 2.3.4 Backdoor** | CVE-2011-2523 | 2.6 – Data Security & Patch Mgmt | ID.RA-01,PR.IP-08 (Vulnerability Mgmt), PR.AC-1 (Access Control) | Annex A 8.8 (Mgmt of Technical Vulnerabilities), Annex A 8.2 (User Access Mgmt), Annex A 8.20 (Network Security Controls) | Art. 32 (Security of Processing), Art. 5(1)(f) (Integrity & Confidentiality) | | **Anonymous FTP Login** | N/A | 2.6 – Data Security & Access Restriction | PR.AC-1, PR.AC-4 (Access Control), PR.PT-3 (Least Privilege) | Annex A.5.15 (Access Control Policy), A.8.2 (User Access Mgmt), Annex A 8.3 (System & App Access Control) | Art. 25 (Data Protection by Design), Art. 32 | | **OpenSSH 4.7p1 (Outdated)** | CVE-2008-5161 | 2.6 – Patch Mgmt | PR.IP-08, PR.PS-05 (Vulnerability Mgmt) | Annex A 8.8 (Technical Vulnerabilities) | Art. 32 | | **Telnet (Plaintext Auth)** | N/A | 2.6 – Secure Communication | PR.DS-2 (Data in Transit), PR.AC-5 (Network Segmentation) | Annex A 5.13 (Info Transfer Policies) | Art. 32 | | **Postfix (SSLv2 Enabled)** | CVE-2011-0411 | 2.6 – Patch Mgmt | PR.DS-2 (Data in Transit Protection) | Annex A 8.24 (Cryptographic Controls), | Art. 32 | | **ISC BIND 9.4.2 (Cache Poisoning)** | CVE-2009-0025 | 2.6 – Patch Mgmt | DE.CM-1 (Monitoring), PR.IP-08 | Annex A 8.8 (Technical Vulnerabilities), Annex A 8.20 (Network Security) | Art. 32 | | **Apache HTTPD 2.2.8 (DoS, RCE)** | CVE-2011-3192 | 2.6 – Patch Mgmt | PR.IP-08, DE.CM-8 (Vulnerability Mgmt & Detection) | Annex A 8.8 (Technical Vulnerabilities), Annex A 8.20 (Network Security) | Art. 32 | | **Samba 3.0.20 (Remote Code Execution)** | CVE-2007-2447 | 2.6 – Patch Mgmt | PR.AC-1, PR.IP-08 | Annex A 8.8 (Technical Vulnerabilities), Annex A 5.15 (Access control), A.8.2 (Privileged access rights), Annex A 8.3 (Access rights to systems and applications) | Art. 32 | | **ProFTPD 1.3.1 (Backdoor, RCE)** | CVE-2010-4221 | 2.6 – Patch Mgmt | PR.AC-1, PR.IP-08 | Annex A 8.8 (Technical Vulnerabilities) | Art. 32 | |  |  |  |  |  |  | | **MySQL 5.0.51a (Auth Bypass)** | CVE-2012-2122 | 2.6 – Patch Mgmt | PR.AA-3, PR.DS-5 (Data Security) | Annex A 8.8 (Technical Vulnerabilities), Annex A 5.15 (Access control), A.8.2 (Privileged access rights), Annex A 8.3 (Access rights to systems and applications) | Art. 32 | | **PostgreSQL 8.3.0 (Priv Escalation)** | CVE-2009-3230 | 2.6 – Patch Mgmt | PR.AA-5 | Annex A 8.8 (Technical Vulnerabilities), | Art. 32 | | **VNC (Weak Authentication)** | N/A | 2.6 – Authentication Security | PR.AA-5, PR.AA-7 (Least Privilege, MFA) | Annex A 5.17 (Authentication Information) | Art. 32 | | **Tomcat 5.5 (Info Disclosure / RCE)** | CVE-2009-3548 | 2.6 – Patch Mgmt | PR.PS-2  DE.CM-03 | Annex A 8.8 (Technical Vulnerabilities) | Art. 32 | | **UnrealIRCd 3.2.8.1 (Backdoor)** | CVE-2010-2075 | 2.6 – Patch Mgmt | PR.PS-2, PR.DS-5 | Annex A 8.8 (Technical Vulnerabilities) | Art. 32 | |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |