**Executive Summary:** Na het uitvoeren van meerdere scans zijn er een paar belangrijke punten uit gekomen waar direct naar gekeken moet worden. De belangrijksten staan hieronder uitgelijnd met alles wat er aan het licht gekomen is en wat eraan gedaan kan worden.

**Gevonden Aandacht Punten**

**1A FTP Service: Poort: 20**

* **Vulnerability**: Anonymous FTP access staat aan, hierdoor kan iedere gebruiker de ftp-server bereiken zonder gebruik te maken van een wachtwoord, wat ertoe lijdt dat iedereen alle bestanden binnen de WWW folder kan bekijken.
* **Risk**: Hoog risico tot het bekijken en downloaden van bestanden wat tot een data lek kan leiden

**1B SSH Service: Poort: 20**

* **Positive** **Configuration**: Support zowel public key als wachtwoord authenticatie, geen zwakke plekken gevonden op eerste aanzicht.

**1C HTTP Service: Poort: 80**

* **Vulnerability**: Gebruikt outdated versie van Apache, dit kan leiden tot mogelijke exploits.
* **Vulnerability**: Gebrek aan http-security headers, zoals “X-Frame-Options" en “X-Content-Type-Options", dit houdt de site open voor aanvallen als clickjacking en MIME type sniffing.
* **Vulnerability**: **info.php** is toegankelijk, dit laat sensitieve PHP-configuratie details zien.
* **Risk**: Hoog door de potentie van bekende en makkelijk uit te voeren aanvallen door misconfiguratie.

**1D MySQL Service:**

* **Vulnerability**: Meerdere gebruiker accounts met mogelijk lege wachtwoorden, waarvan veel accounts hoge privilege niveaus hebben.
* **Positive Configuration**: MySQL heeft een gelimiteerd aantal pogingen om in te loggen aanstaan. Dit maakt het risico op “brute-force” aanvallen minder.
* **Risk**: Mogelijk maar ongetoetst lek afhankelijk van of de MySQL accounts inderdaad geen wachtwoord nodig zijn wat kan leiden tot onbevoegd toegang tot de databases.

**1E Server File Permissions:**

* **Positive Configuration**: Read en Write bestands rechten zijn volgens de norm ingesteld, met wel mogelijk problemen mocht iemand toegang krijgen tot account WWW-Data.
* **Risk**: Moderate. Hoewel de bestands rechten goed ingesteld staan kan het een probleem worden mocht iemand toegang krijgen tot WWW-Data.

**1F PHP Configuration:**

* **Vulnerability**: variabele “**open\_basedir”** is niet ingesteld, wat de optie openzet om PHP-scripts te kunnen uitvoeren en toegang te krijgen tot bestanden buiten de WWW folder.
* **Risk**: Hoog wanneer gecombineerd met bekende exploits zoals “LFI” (Local File Inclusion).

**1G SIP Configuration:**

* **VoIP Services**: Geen problemen gevonden betreffende de SCCP en de SIP poorten tijden dit assessment.

**Overall Security Posture:**

Het geteste systeem laat een mix zien van goed geconfigureerde software met een paar vrij bekende beginnersfouten die grote problemen kunnen veroorzaken. Hierdoor raden we aan direct de volgende dingen uit te voeren en hierna een het assessment uit te laten voeren om te kijken of de mogelijke lekken nu dicht zijn.

**Recommendations:**

* Zet anonymous ftp-access uit zoals omschreven in 1A
* Update Apache naar de nieuwste stabiele versie en zet de security headers aan zoals omschreven in 1C
* Verwijder **info.php** uit de productie omgeving zoals omschreven in 1C.
* Controleer of MySQL gebruikers accounts geen wachtwoord hebben. Mocht dit het geval zijn zorg dat deze een wachtwoord krijgen.
* Stel “**open\_basedir”** in de configuratie van PHP om toegang tot bestanden via PHP-scripts te limiteren.

**Conclusion:** Zoals uitgelijnd in dit document zijn er een paar aandacht punten die direct behandeld moeten worden. Na het uitvoeren van deze veranderingen is het van belang om nog een test uit te laten voeren om te kijken of deze veranderingen goed doorgevoerd zijn zoals omschreven in dit rapport.

**Mogelijk Handige Linkjes:**

* Anonymous FTP uitzetten: <https://wiki.centos-webpanel.com/disable-anonymous-login-on-pure-ftp-server>
* Update Apache: <https://httpd.apache.org/docs/2.4/upgrading.html>
* Verwijder Info.php: <https://docs.backdropcms.org/documentation/enabling-and-disabling-phpinfo>