FortifyTech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

Dokumen ini adalah milik eksklusif FortifyTech dan Cybershield. Dokumen ini berisi informasi hak milik dan rahasia. Duplikasi, distribusi ulang, atau penggunaan, secara keseluruhan atau sebagian, dalam bentuk apa pun, memerlukan persetujuan dari .

Demo Corp dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan terhadap persyaratan uji penetrasi.

Disclaimer

Uji penetrasi dianggap sebagai snapshot dalam waktu tertentu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

Keterlibatan yang dibatasi waktu tidak memungkinkan untuk evaluasi penuh terhadap semua kontrol keamanan. Cybershield memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan terlemah yang akan dieksploitasi oleh penyerang. Cybershield merekomendasikan untuk melakukan penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan kontrol yang berkelanjutan.

Contact Information

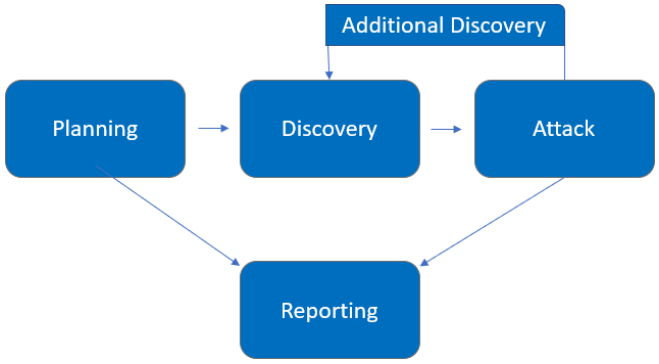
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
Cybershield		
Rahmad Aji W.	Penetration Tester	Email: aji.wicaksono18@gmail.com

Assessment Overview

Dari 5 hingga 8 Mei 2024, FortifyTech melibatkan Cybershield untuk mengevaluasi postur keamanan infrastrukturnya dibandingkan dengan praktik terbaik industri saat ini yang mencakup uji penetrasi jaringan internal. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis NIST SP 800-115 untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka kerja pengujian yang disesuaikan.

Tahapan kegiatan pengujian penetrasi meliputi hal-hal berikut:

- Perencanaan - Tujuan pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Penemuan - Melakukan pemindaian dan pencacahan untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Serangan - Mengkonfirmasi potensi kerentanan melalui eksploitasi dan melakukan penemuan tambahan pada akses baru.
- Pelaporan - Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Assessment Components

Internal Penetration Test

Uji penetrasi internal mengemulasi peran penyerang dari dalam jaringan. Seorang teknisi akan memindai jaringan untuk mengidentifikasi potensi kerentanan host dan melakukan serangan jaringan internal yang umum dan canggih, seperti: Peracunan LLMNR/NBT-NS dan serangan man-in-the-middle lainnya, peniruan token, kerberoasting, pass-the-hash, golden ticket, dan banyak lagi. Peretas akan berusaha mendapatkan akses ke host melalui pergerakan lateral, mengkompromikan akun pengguna dan admin domain, dan mengeksfiltrasi data sensitif.

Finding Severity Ratings

Tabel berikut ini mendefinisikan tingkat keparahan dan rentang skor CVSS yang sesuai yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksploitasi sangat mudah dan biasanya menghasilkan kompromi tingkat sistem. Disarankan untuk membuat rencana tindakan dan segera menambalnya.
High	7.0-8.9	Eksploitasi lebih sulit tetapi dapat menyebabkan peningkatan hak istimewa dan berpotensi kehilangan data atau waktu henti. Disarankan untuk membuat rencana tindakan dan menambal sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah ekstra seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan menambal selama masa pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Risk Factors

Risiko diukur dengan dua faktor: Likelihood dan Impact:

Likelihood

Likelihood mengukur potensi kerentanan yang dieksploitasi. Peringkat diberikan berdasarkan tingkat kesulitan serangan, alat yang tersedia, tingkat keahlian penyerang, dan lingkungan klien.

Impact

Impact mengukur dampak kerentanan potensial terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerugian reputasi, dan kerugian

finansial.

Scope

Assessment	Details
Internal Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

Sesuai permintaan klien, TCMS tidak melakukan salah satu dari serangan berikut ini selama pengujian:

- Denial of Service (DoS)
- Phishing/Social Engineering
- Hindari hal - hal yang melanggar etika

Semua serangan lain yang tidak disebutkan di atas diizinkan oleh FortifyTech.

Client Allowances

Demo Corp memberikan TCMS akses berikut ini:

- Internal akses ke jaringan ITS via VPN.

Executive Summary

Cybershield mengevaluasi postur keamanan internal FortifyTech melalui pengujian penetrasi dari 5 hingga 8 Mei 2024. Bagian berikut memberikan gambaran umum tingkat tinggi tentang kerentanan yang ditemukan, upaya yang berhasil dan tidak berhasil, serta kekuatan dan kelemahan.

Scoping and Time Limitations

Pelingkupan selama penugasan tidak mengizinkan penolakan layanan atau rekayasa sosial di semua komponen pengujian.

Batasan waktu yang ditetapkan untuk pengujian. Pengujian penetrasi jaringan internal diizinkan selama tiga (3) hari.

Testing Summary

Didapatkan bahwa sebuah celah pada port 8888 dan 21 di mana port 8888 dapat mengakses halaman login sedangkan pada port 21 ketika dicek menggunakan nmap dapat diketahui yaitu terdapat login ftp secara anonim. Setelah dapat masuk melalui ftp secara anonim pada port 21 didapatkan file backup.sql saat melihat direktori menggunakan ls -la.

Tester Notes and Recommendations

1. Penutupan Celah Keamanan:
    - Segera perbaiki celah pada port 8888. Pastikan bahwa akses ke halaman login hanya dapat dilakukan oleh pengguna yang sah dan telah diotentikasi.
    - Pertimbangkan untuk memperbarui atau mengkonfigurasi ulang server web untuk mengurangi risiko akses tidak sah.
2. Perlindungan FTP:
    - Matikan login FTP anonim atau setidaknya batasi akses ke direktori tertentu. Ini akan mencegah akses tidak sah ke file sensitif.
    - Jika login anonim diperlukan untuk tujuan tertentu, pastikan hanya file yang perlu diakses oleh publik yang tersedia, dan file-file sensitif tidak dapat diakses.
3. Manajemen File Backup:
    - Periksa isi dari file backup.sql untuk memastikan tidak ada informasi sensitif yang terpapar.
    - Segera hapus file backup.sql jika tidak diperlukan lagi atau pindahkan ke tempat yang lebih aman jika masih dibutuhkan.

Key Strengths and Weaknesses

Berikut ini adalah identifikasi kekuatan utama yang diidentifikasi selama penilaian:

1. Keberhasilan dalam mendeteksi celah keamanan pada port 8888 dan port 21 menunjukkan kepekaan terhadap keamanan sistem.
2. Ketersediaan informasi tentang celah keamanan dan file sensitif menunjukkan adanya kesadaran keamanan di dalam organisasi atau tim.
3. Pemindaian menggunakan nmap menunjukkan kemampuan untuk mengidentifikasi dan mengaudit layanan yang terbuka di server.
4. Kemampuan untuk memahami informasi teknis seperti penggunaan FTP anonim, penggunaan nmap, dan penanganan file backup.sql menunjukkan tingkat pemahaman yang baik terhadap teknologi.

The following identifies the key weaknesses identified during the assessment:

1. Adanya celah keamanan pada port 8888 menunjukkan kurangnya pembaruan atau pengelolaan yang tepat terhadap konfigurasi server web.
2. Penggunaan FTP anonim dapat membuka pintu bagi serangan dan akses tidak sah ke file sensitif.
3. Penemuan file backup.sql menunjukkan kurangnya kebijaksanaan dalam manajemen file backup, karena file tersebut mungkin berisi informasi sensitif dan tidak seharusnya terbuka untuk akses publik.
4. Ketergantungan pada alat pemindaian seperti nmap dapat menunjukkan kurangnya pemantauan proaktif terhadap keamanan sistem secara terus-menerus tanpa harus bergantung pada alat eksternal.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

1	1	0	0	1
Critical	High	Moderate	Low	Informational

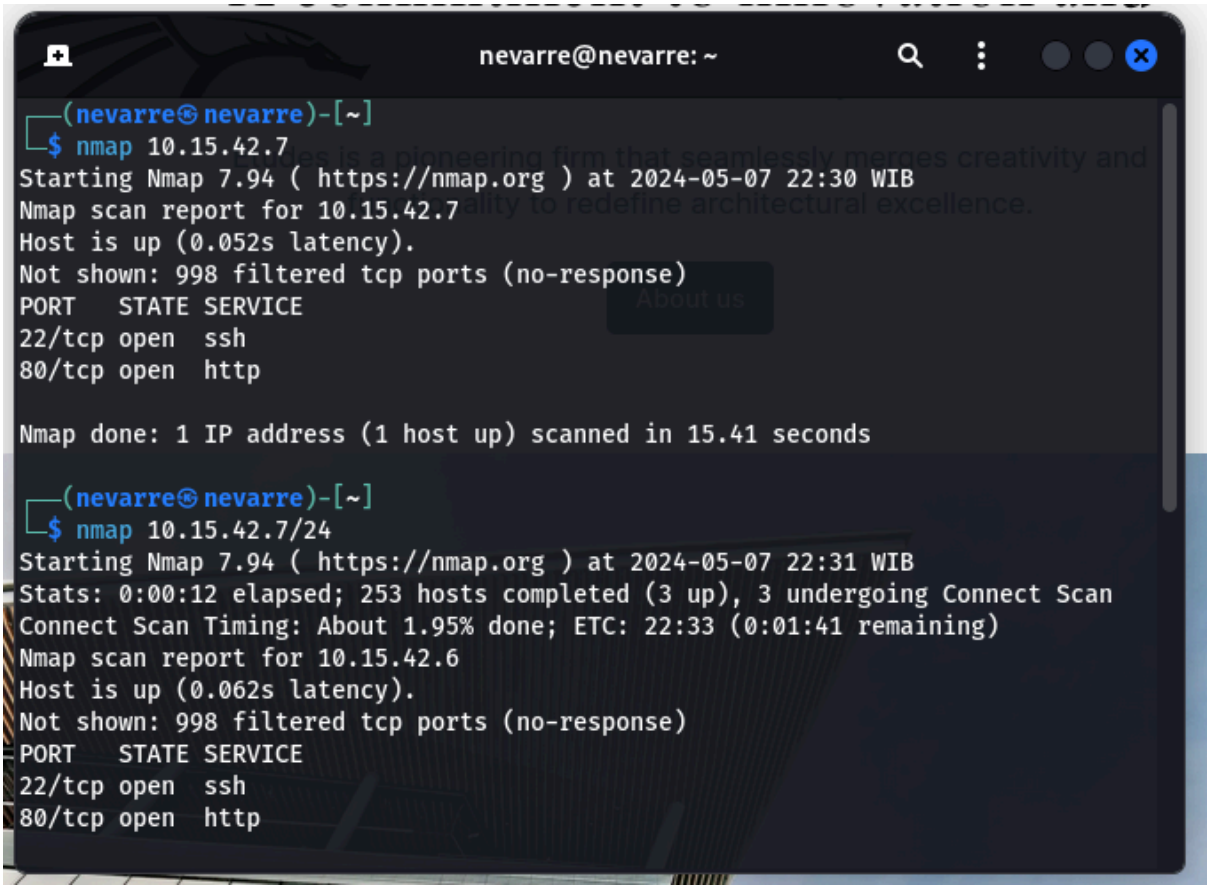
Finding	Severity	Recommendation
Internal Penetration Test		
CVE-1999-0497: FTP Anonymous Login	Critical	Apply the appropriate Microsoft patches to remediate the issue.

Finding	Severity	Recommendation
CVE-2022-0255:Backup.sql	High	Use Group Managed Service Accounts (GMSA) for privileged services.
Steps to Domain Admin	Informational	Review action and remediation steps.

Technical Findings

Internal Penetration Test Findings

1. Scan nmap

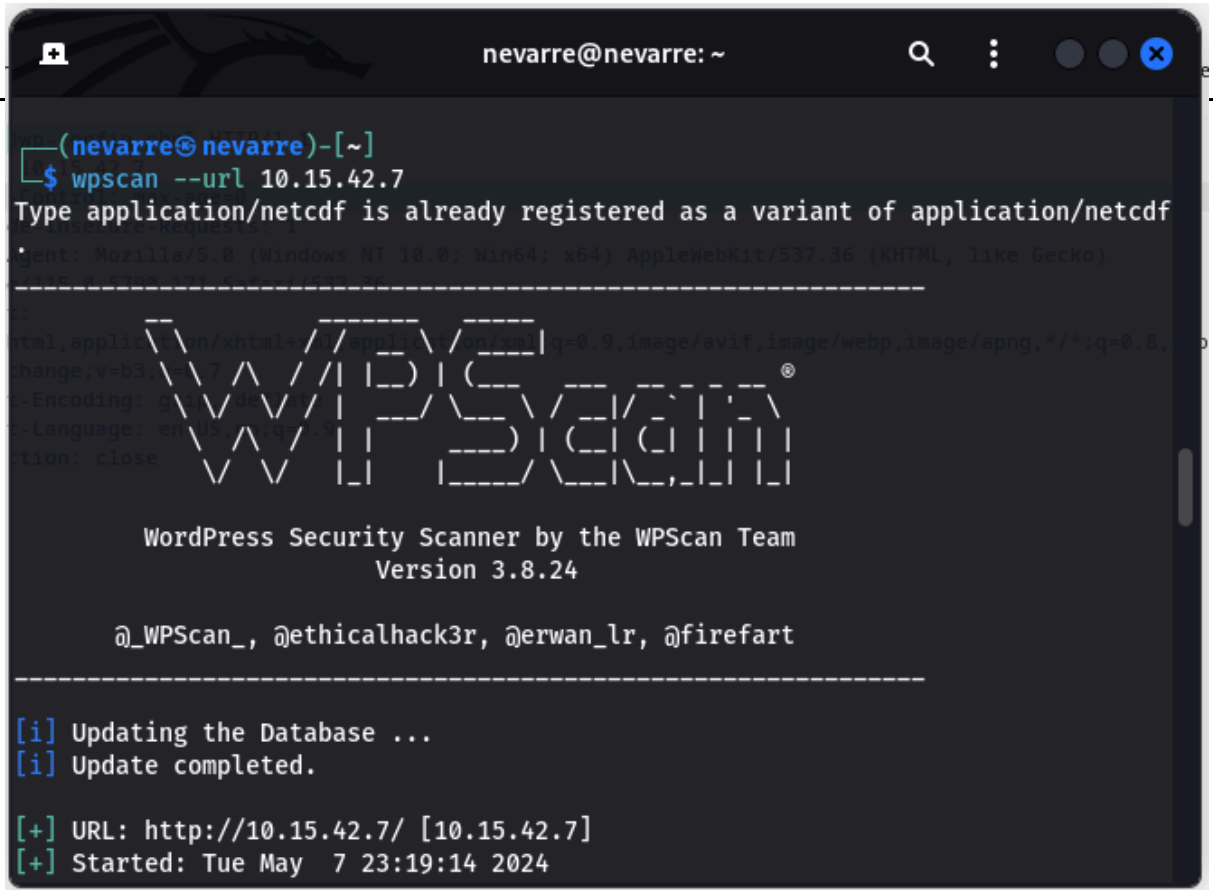


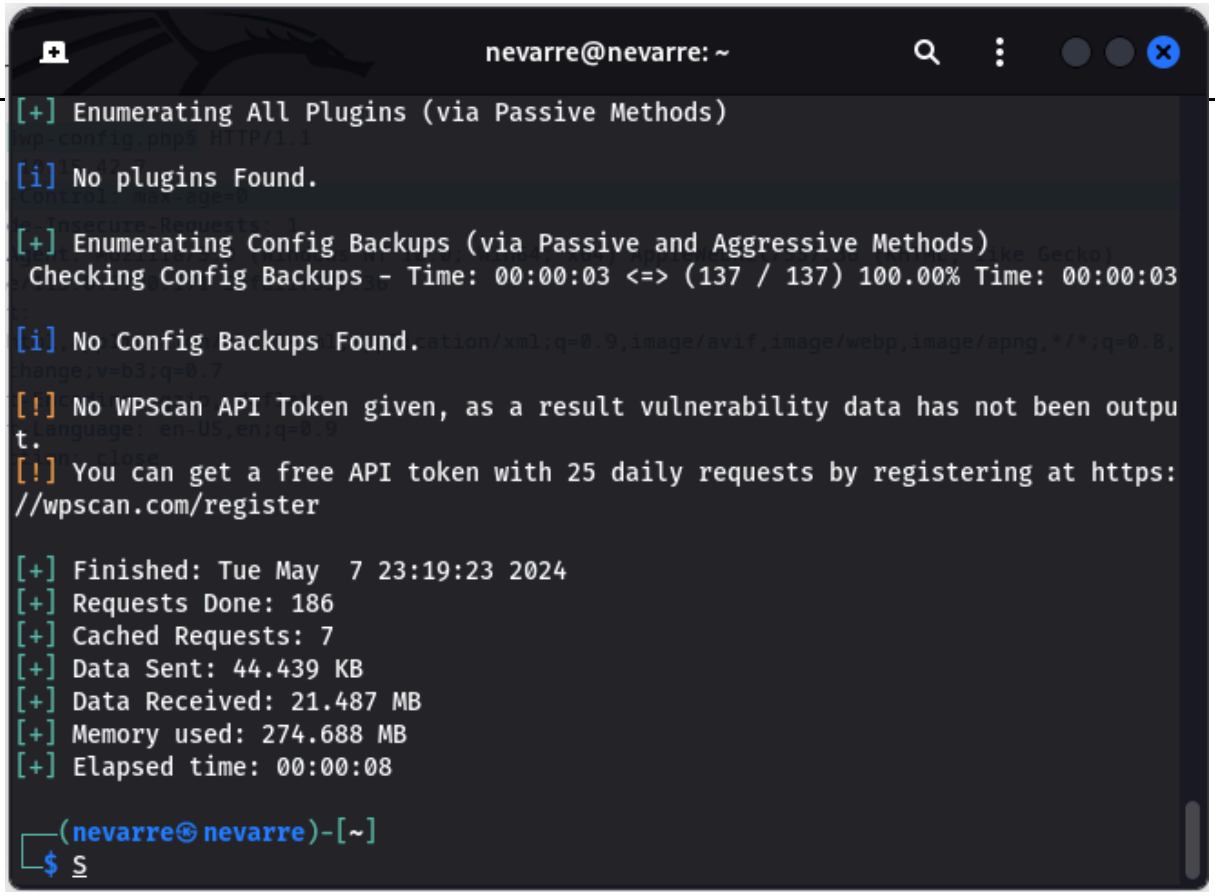

```
┌──(nevarre㉿nevarre)-[~/Downloads]
└─$ nmap -p- -T4 10.15.42.36 -Pn | tee open_ports
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 19:54 WIB
Nmap scan report for 10.15.42.36
Host is up (0.059s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
8888/tcp open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 241.89 seconds
```

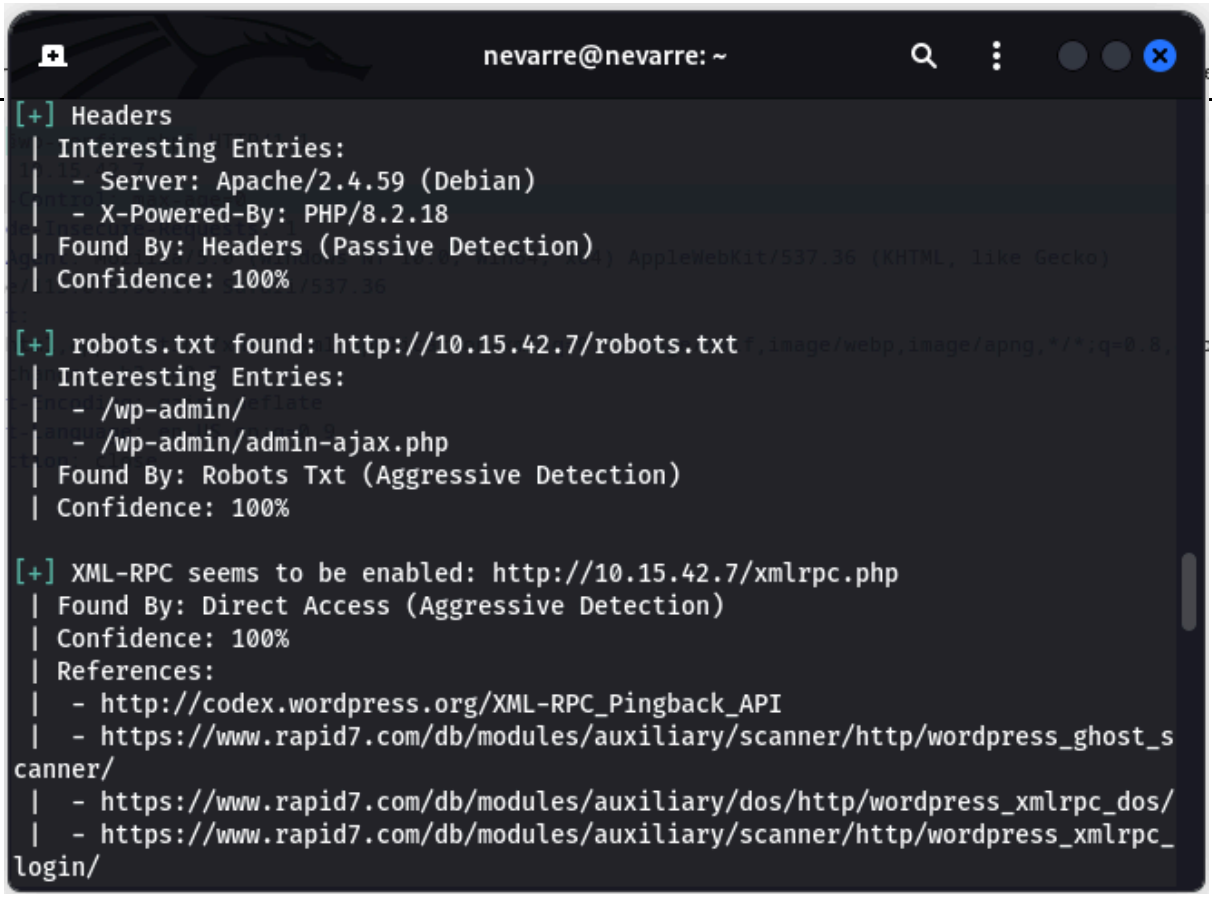
```
┌──(nevarre㉿nevarre)-[~/Downloads]
└─$ sudo nmap -sS -sV -A -O -p21,22,139,445 10.15.42.36 | tee port_details
[sudo] password for nevarre:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 20:00 WIB
SSNmap scan report for 10.15.42.36
Host is up (0.0058s latency).

PORT    STATE    SERVICE      VERSION
21/tcp  open     ftp          vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.4.213
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
```

```
┌──(nevarre㉿nevarre)-[~/Downloads]
└─$ nmap -oN nmaplog.log 10.15.42.36 -A -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-08 20:02 WIB
Nmap scan report for 10.15.42.36
Host is up (0.052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.29 seconds
```

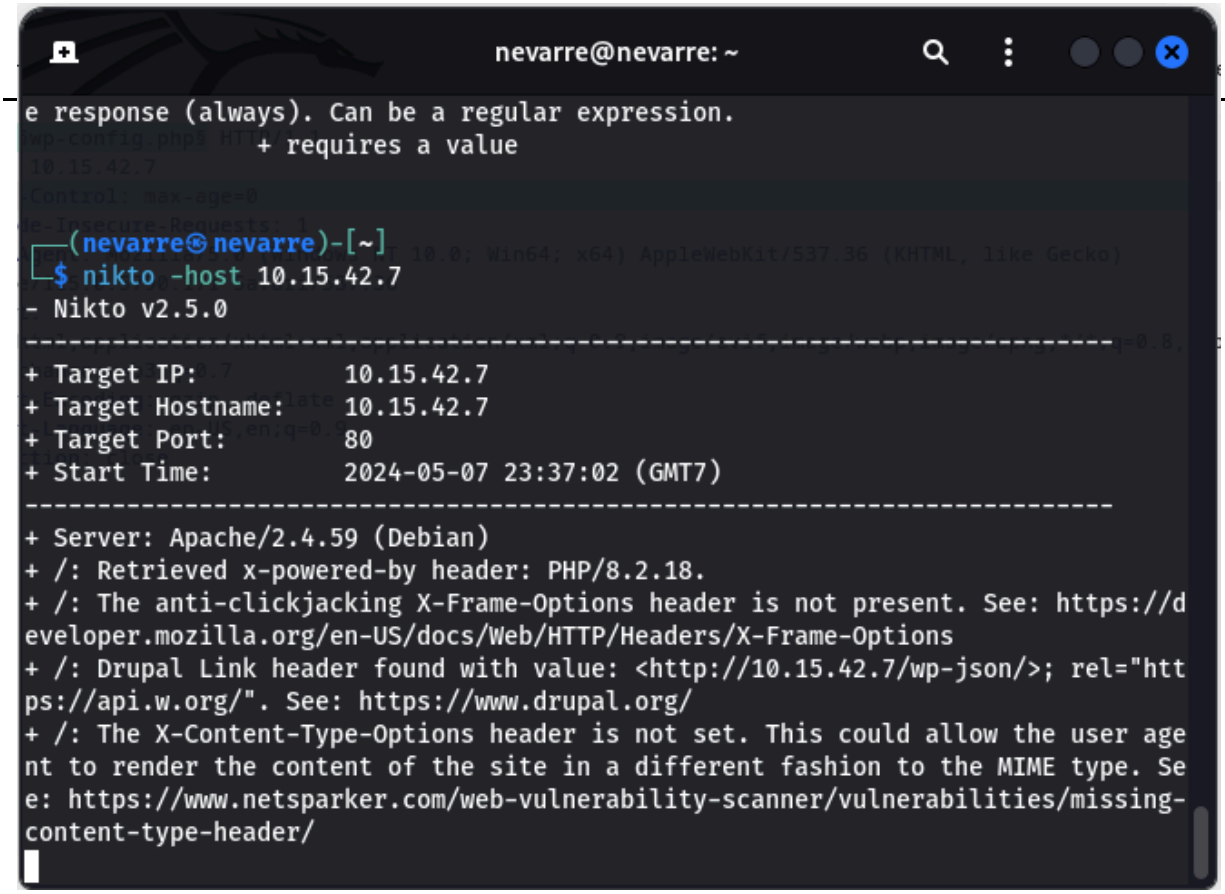
WPScan


nevarre@nevarre: ~
(nevarre㉿nevarre)-[~]
$ wpscan --url 10.15.42.7
Type application/netcdf is already registered as a variant of application/netcdf
.
WordPress Security Scanner by the WPScan Team
Version 3.8.24
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://10.15.42.7/ [10.15.42.7]
[+] Started: Tue May 7 23:19:14 2024

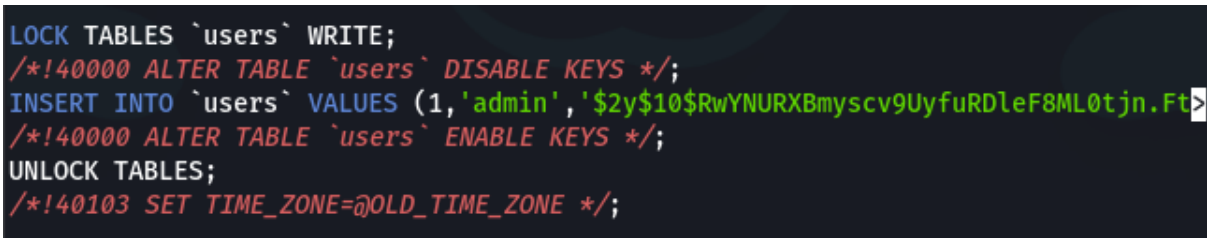

nevarre@nevarre: ~
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:03 <=> (137 / 137) 100.00% Time: 00:00:03
[i] No Config Backups Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Tue May 7 23:19:23 2024
[+] Requests Done: 186
[+] Cached Requests: 7
[+] Data Sent: 44.439 KB
[+] Data Received: 21.487 MB
[+] Memory used: 274.688 MB
[+] Elapsed time: 00:00:08
(nevarre㉿nevarre)-[~]
$ S


nevarre@nevarre: ~
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.59 (Debian)
| - X-Powered-By: PHP/8.2.18
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] robots.txt found: http://10.15.42.7/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://10.15.42.7/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

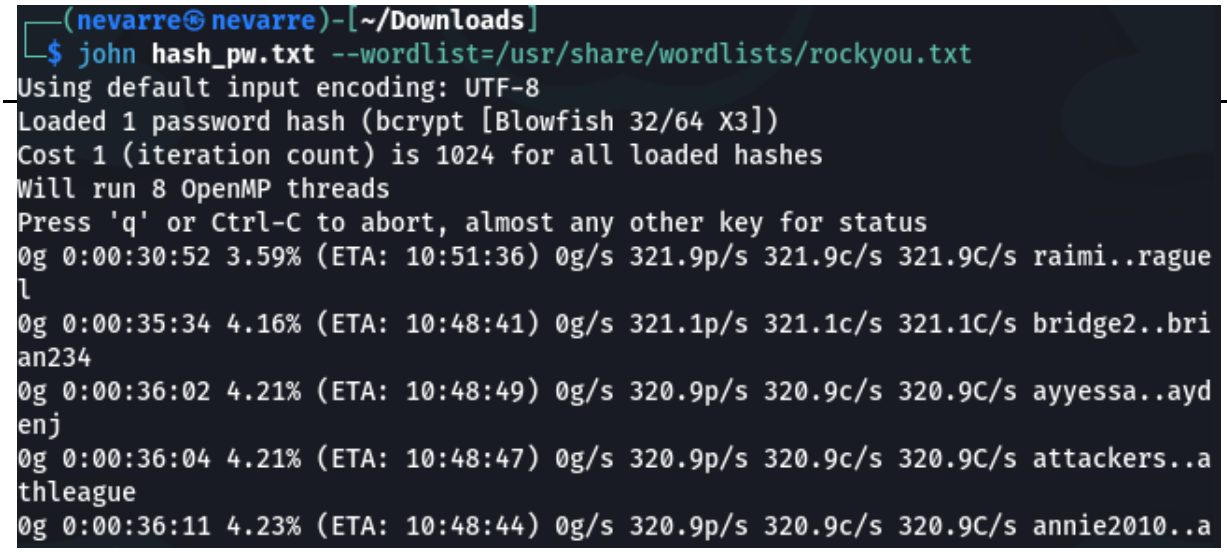
nikto



isi backup.sql ftp anonymous login



percobaan decrypt hash password dengan john the ripper



Remediation

Review action and remediation steps.

Additional Scans and Reports

Cybershield menyediakan semua informasi laporan yang dikumpulkan selama pengujian kepada semua klien. Ini termasuk file Nessus dan pemindaian kerentanan penuh dalam format terperinci. Laporan-laporan ini berisi pemindaian kerentanan mentah dan kerentanan tambahan yang tidak dieksploitasi oleh Cybershield.

Laporan tersebut mengidentifikasi masalah kebersihan yang perlu diperhatikan tetapi kecil kemungkinannya untuk mengarah pada pelanggaran, yaitu peluang pertahanan yang mendalam. Untuk informasi lebih lanjut, lihat dokumen di folder drive bersama Anda yang berlabel "Pemindaian dan Laporan Tambahan".

Last Page