DEMO CORP
Security Assessment Findings Report

Business Confidential

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

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
Demo Corp		
Agas Ananta Wijaya	Praktikum 2 Ethical Hacking	Email: agasananta04@gmail.com
TCM Security		
Aslab Teknologi Informasi ITS	Lead Penetration Tester	Email: -

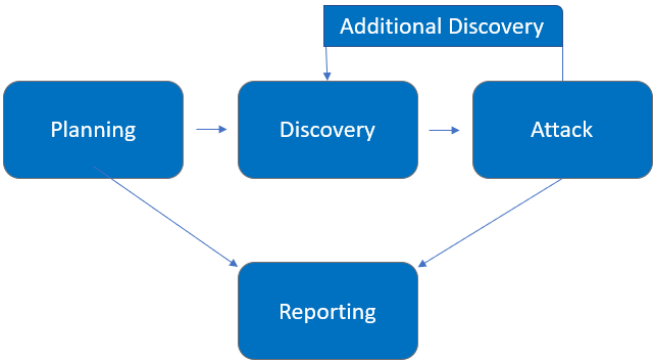
Assessment Overview

Kita para praktikan praktikum ethical hacking Teknologi Informasi ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka.

Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Blackbox Pentest	10.15.42.36 10.15.42.7

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

Demo Corp provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Kita para praktikan praktikum ethical hacking Teknologi Informasi ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka.

Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

Technical Findings

Internal Penetration Test Findings

Mencari Port dari masing masing IP menggunakan NMAP

Description:	Mencari port yang terbuka merupakan salah satu langkah penting dalam ethical hacking karena memberikan informasi awal tentang sistem yang menjadi target. Port yang terbuka dapat memberikan petunjuk tentang layanan atau aplikasi yang berjalan di dalam sistem. mencari port yang terbuka menjadi langkah kritis dalam proses ethical hacking karena membantu dalam pemahaman yang lebih baik tentang sistem yang sedang diserang dan memungkinkan identifikasi dan penilaian potensi kerentanan serta titik masuk bagi attacker.
Risk:	Scanning port yang intensif atau agresif dapat menghasilkan beban tambahan pada jaringan atau sistem target, yang mungkin menyebabkan penurunan kinerja atau bahkan gangguan layanan. Beberapa sistem keamanan dapat mendeteksi aktivitas scanning port yang mencurigakan dan merespons dengan memblokir alamat IP attacker atau memberi peringatan kepada administrator jaringan.
System:	All
Tools Used:	Nmap
References:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidence

```
┌──[root@parrot]─[~]
└──╼ #cat port_36
# Nmap 7.94SVN scan initiated Wed May  8 16:05:32 2024 as: nmap -sS -oN port_36
10.15.42.36
Nmap scan report for 10.15.42.36
Host is up (0.0024s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
8888/tcp open  sun-answerbook

# Nmap done at Wed May  8 16:05:38 2024 -- 1 IP address (1 host up) scanned in 5
.96 seconds
```

Figure 1: Mencari Port yang terbuka dari IP 10.15.42.36

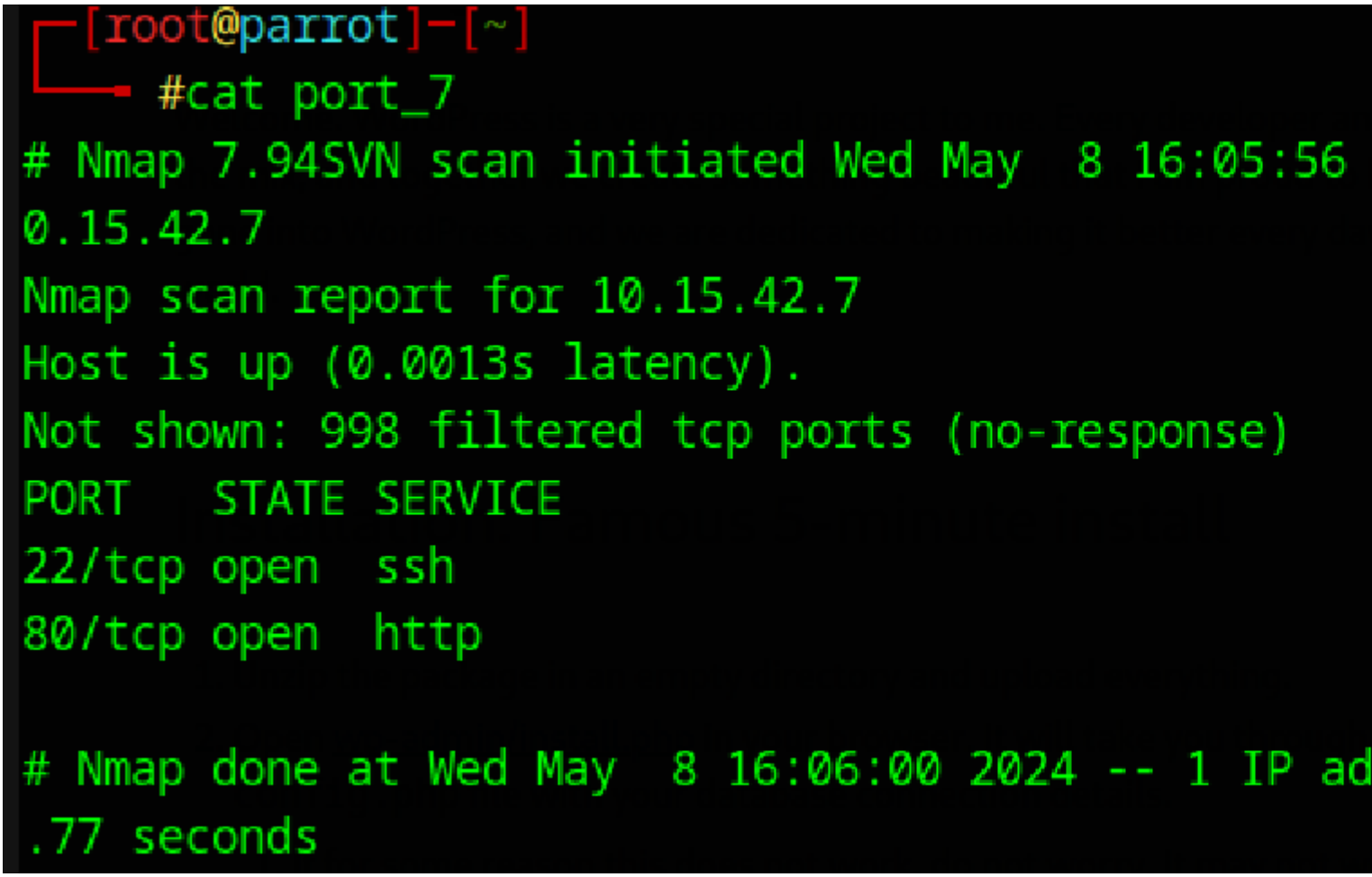


Figure 2: Mencari Port yang terbuka dari IP 10.15.42.7

Remediation

Setelah melakukan scanning port menggunakan NMAP dan mengidentifikasi layanan yang berjalan di tiap alamat IP, langkah selanjutnya adalah merencanakan tindakan remediasi yang sesuai untuk meningkatkan keamanan sistem.

Untuk Alamat IP 10.15.42.36:

1. **FTP (Port 21)**: Kita harus memeriksa konfigurasi FTP server untuk memastikan bahwa akses tidak dibiarkan terbuka ke direktori sensitif.
2. **SSH (Port 22)**: Kita harus memastikan SSH server diaktifkan dengan konfigurasi keamanan yang ketat.
3. **Sun Answerbook (Port 8888)**: Kita harus memeriksa apakah layanan Sun Answerbook ini memang dibutuhkan.

Untuk Alamat IP 10.15.42.7:

1. **SSH (Port 22)**: Kita harus memastikan untuk memperbarui pengaturan default seperti port SSH yang digunakan, autentikasi dua faktor jika memungkinkan, dan membatasi akses hanya untuk user yang diotorisasi.
2. **HTTP (Port 80)**: Kita harus memeriksa konfigurasi server web untuk memastikan bahwa tidak ada kerentanan keamanan yang dapat dieksploitasi.

Mencari direktori menggunakan Gobuster

Description:	Direktori yang terbuka dapat menjadi sumber potensi kerentanan keamanan, seperti direktori yang tidak diotentikasi, direktori yang tidak diotorisasi, atau direktori yang memiliki izin akses yang salah. Beberapa aplikasi web mungkin memiliki halaman atau fitur yang tidak terdaftar secara terang-terangan di navigasi publik. Dengan menggunakan alat seperti Gobuster, kita dapat menemukan halaman-halaman tersembunyi tersebut. Direktori yang terbuka dapat menjadi sasaran serangan brute force untuk mencari tahu halaman login, API, atau titik akhir lainnya yang dapat dieksploitasi.
Risk:	Gobuster dapat membuat banyak permintaan ke server, terutama jika menggunakan wordlist besar atau melakukan scanning yang luas. Ini bisa menyebabkan kelebihan beban pada server target atau infrastruktur jaringan. Penggunaan Gobuster dapat terdeteksi oleh sistem keamanan seperti firewall atau sistem deteksi intrusi (IDS), terutama jika terlalu agresif atau jika dilakukan dalam jumlah besar.
System:	All
Tools Used:	Gobuster
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence

```
gobuster dir -u http://10.15.42.36:8888/ -w
/usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.36:8888/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
/usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php           (Status: 200) [Size: 603]
/dashboard.php       (Status: 302) [Size: 0] [--> login.html]
Progress: 5163 / 5164 (99.98%)
===============================================================
Finished
===============================================================
```

Figure 3: Hasil pencarian direktori pada IP 10.15.42.36 port 8888

```
gobuster dir -u http://10.15.42.7/ -w
/usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.15.42.7/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:
/usr/share/seclists/Discovery/Web-Content/Common-PHP-Filenames.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php           (Status: 301) [Size: 0] [--> http://10.15.42.7/]
/login.php           (Status: 302) [Size: 0] [--> http://10.15.42.7/wp-login.php]
/xmlrpc.php          (Status: 405) [Size: 42]
Progress: 5163 / 5164 (99.98%)
===============================================================
Finished
===============================================================
```

Figure 4: Hasil pencarian direktori pada IP 10.15.42.7

Remediation

Setelah kita melakukan scanning direktori menggunakan gobuster, kita bisa melakukan scanning vulnerability. Saya menggunakan nuclei untuk melakukan scanning vulnerability

Scanning Vulnerability menggunakan Nuclei

Description:	Nuclei merupakan alat yang sangat berguna bagi para profesional keamanan dalam upaya mereka untuk mengidentifikasi, mengevaluasi, dan memperbaiki kerentanan serta celah keamanan dalam sistem dan aplikasi. Nuclei memungkinkan otomatisasi dalam proses pengujian keamanan, menghemat waktu dan usaha yang diperlukan untuk mencari kerentanan dan celah keamanan secara manual. Nuclei mendukung berbagai jenis scanning, termasuk HTTP, DNS, dan banyak lagi. Ini memungkinkan user untuk menyesuaikan pendekatan mereka sesuai dengan kebutuhan dan tujuan pengujian.
Risk:	Terkadang, alat scanning seperti Nuclei dapat salah mengidentifikasi kerentanan atau celah keamanan, menghasilkan informasi yang tidak akurat atau menyesatkan. Hal ini dapat mengarah pada tindakan perbaikan yang tidak tepat atau tidak efektif.
System:	All
Tools Used:	Nuclei
References:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/

Evidence

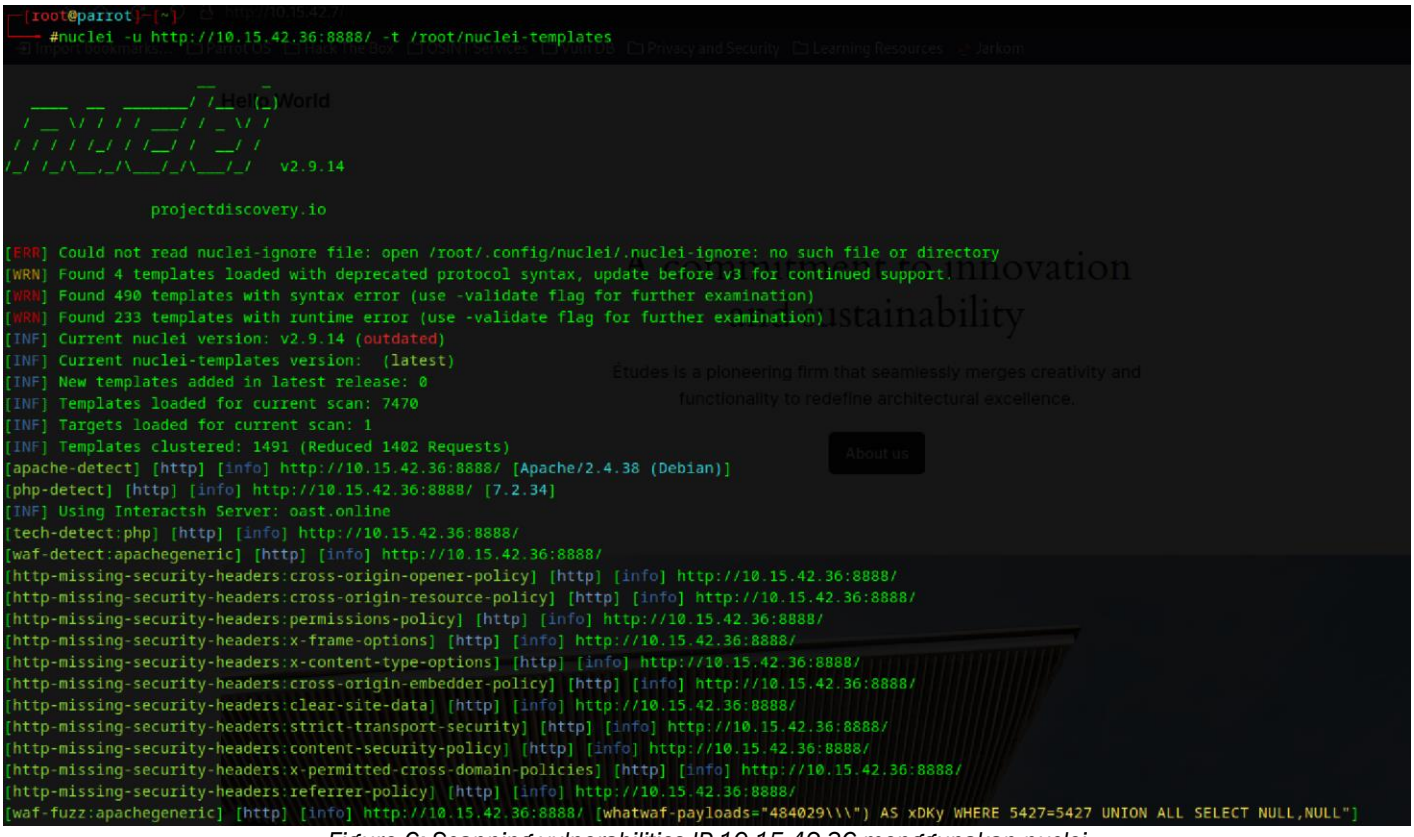


Figure 6: Scanning vulnerabilities IP 10.15.42.36 menggunakan nuclei

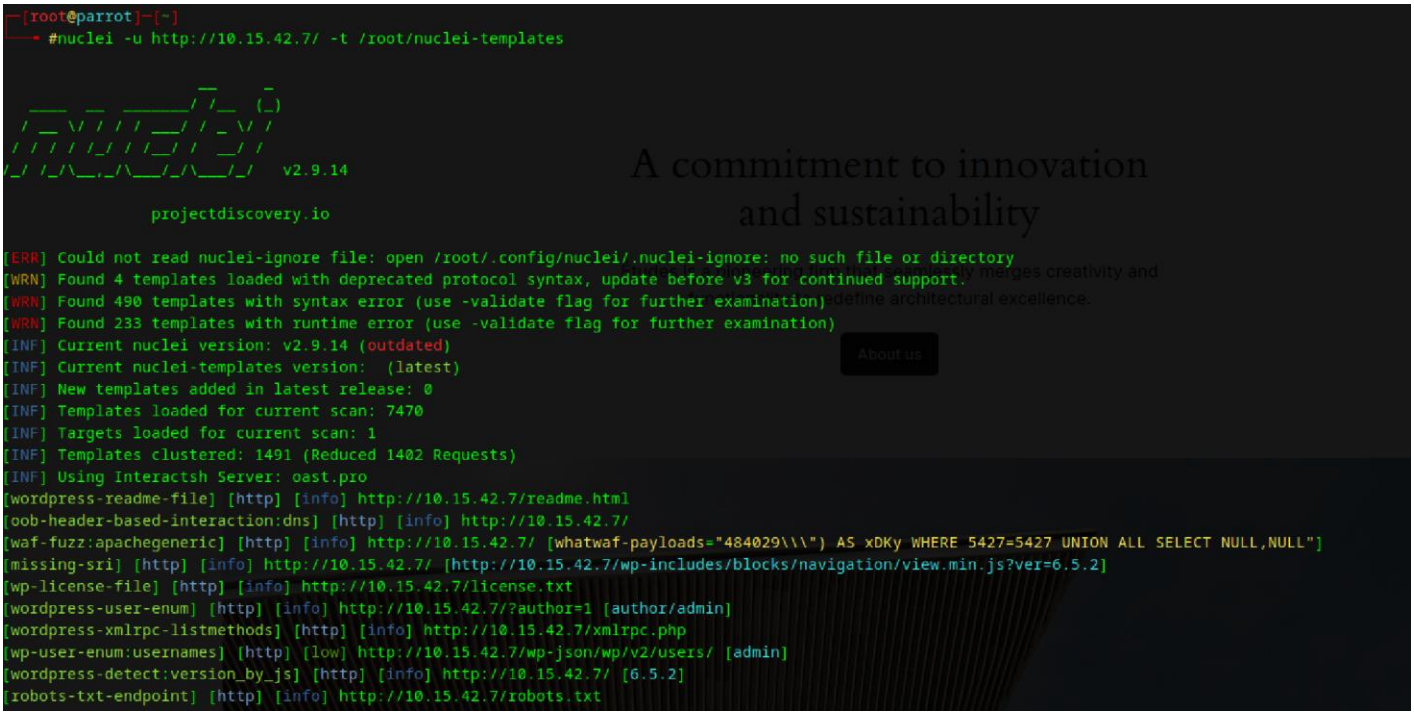


Figure 7: Scanning vulnerabilities IP 10.15.42.7 menggunakan nuclei

Security Strengths

Berdasarkan Figure 6, situs web mungkin rentan terhadap serangan yang memanfaatkan versi perangkat lunak yang telah diketahui, kurangnya header keamanan HTTP, dan kemungkinan kelemahan dalam konfigurasi atau perlindungan WAF. Diperlukan tindakan remediasi seperti memperbarui perangkat lunak, mengkonfigurasi header keamanan yang tepat, dan memeriksa dan memperbarui aturan WAF untuk mengurangi risiko keamanan. Situs web berjalan di server Apache versi 2.4.38 dan menggunakan PHP versi 7.2.34. Informasi ini dapat digunakan oleh attacker untuk mencari kerentanan yang diketahui atau eksploitasi yang spesifik untuk versi perangkat lunak tersebut. Terdeteksi adanya payload yang mencurigakan pada fitur WAF (Web Application Firewall), yang mungkin menunjukkan bahwa situs web rentan terhadap serangan fuzzing atau serangan input yang tidak valid.

Berdasarkan Figure 7, ditemukan readme.html, license.txt, dan xmlrpc.php menunjukkan bahwa situs web di IP 10.15.42.7 berjalan pada platform WordPress. Informasi ini memberikan petunjuk kepada attacker bahwa situs web rentan terhadap serangan yang spesifik terhadap platform WordPress. Lalu juga ditemukan seperti wp-user-enum:usernames dan wordpress-user-enum memberikan informasi tentang user yang ada di situs web WordPress tersebut. Ini dapat memberikan attacker akses ke informasi penting tentang user, seperti nama user (username), yang dapat digunakan untuk mencoba serangan brute-force atau serangan phishing. Situs web WordPress pada IP 10.15.42.7 rentan terhadap serangan seperti eksploitasi informasi user, serangan kelemahan versi, serangan luar jalur, dan manipulasi sumber daya. Tindakan remediasi yang diperlukan termasuk memperbarui WordPress dan plugin yang digunakan, mengonfigurasi kebijakan keamanan yang tepat, dan memeriksa kelemahan yang diketahui yang mungkin ada pada versi WordPress dan plugin yang digunakan.

Additional Scans and Reports

Berdasarkan informasi yang diberikan dari hasil scanning tersebut, kita dapat menarik kesimpulan sebagai berikut:

IP 10.15.42.36:

1. Kerentanan:
   - FTP server memungkinkan akses anonim, yang berpotensi membuka risiko kebocoran informasi sensitif.
   - Versi SSH yang digunakan mungkin rentan terhadap serangan yang diketahui atau telah diperbaiki dalam versi yang lebih baru.
   - Versi Apache HTTP Server yang digunakan mungkin rentan terhadap serangan yang diketahui jika tidak diperbarui dengan patch keamanan terbaru.
2. Remediasi:
   - Memperbarui semua perangkat lunak yang digunakan ke versi terbaru dengan patch keamanan.
   - Mengonfigurasi server FTP dan SSH dengan kebijakan keamanan yang ketat, termasuk penggunaan autentikasi yang kuat dan akses yang terbatas.
   - Memantau dan mengelola konfigurasi keamanan Apache HTTP Server untuk menghindari kebocoran informasi sensitif atau eksploitasi kerentanan yang diketahui.

IP 10.15.42.7:

1. Kerentanan:
   - Server HTTP (mungkin WordPress) teridentifikasi dengan beberapa kerentanan potensial, termasuk:
     - Kemungkinan adanya berkas readme yang dapat memberikan informasi sensitif tentang instalasi WordPress.
     - Eksploitasi potensial terkait dengan protokol XML-RPC yang dapat dieksploitasi oleh penyerang.
     - Kemungkinan eksploitasi terkait dengan konfigurasi keamanan yang buruk, seperti ketidakhadiran beberapa header keamanan HTTP.
     - Kemungkinan pengungkapan informasi sensitif melalui berkas lisensi WordPress dan robot.txt.
2. Remediasi:
   - Memperbarui WordPress dan plugin yang digunakan ke versi terbaru.
   - Menghapus berkas readme, berkas lisensi, dan informasi sensitif lainnya dari server.
   - Memperbaiki konfigurasi keamanan pada server web, termasuk penggunaan header keamanan HTTP yang tepat.
   - Memantau dan memeriksa secara teratur kerentanan baru serta memastikan bahwa sistem tetap diperbarui dengan patch keamanan terbaru.

Last Page