ForityTech
Security Assessment Findings Report

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

Confidentiality Statement

Dokumen ini merupakan milik eksklusif dari FortifyTech dan CyberShield. Dokumen ini berisi informasi properti dan rahasia yang bersifat rahasia. Penyalinan, redistribusi, atau penggunaan, secara keseluruhan atau sebagian, dalam bentuk apapun, memerlukan persetujuan dari kedua FortifyTech dan CyberShield.
FortifyTech dapat membagikan dokumen ini kepada pihak auditor di bawah perjanjian rahasia untuk menunjukkan kepatuhan terhadap persyaratan uji penetrasi.

Disclaimer

Segala bentuk kegiatan *reconnaissance* (pengintaian) tanpa izin pada pemilik layanan/sistem dapat dikenakan **sanksi pidana yang serius**. Segala informasi yang dipaparkan di sini **hanya untuk tujuan pembelajaran** dan **tidak boleh** digunakan untuk aktivitas ilegal.

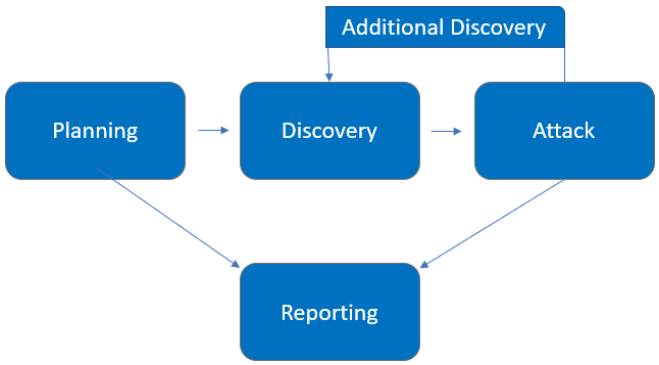
Contact Information

Name	Title	Contact Information
Stephanie	Mahasiswa IT 22	Email: heath@tcm-sec.com

Assessment Overview

Dari tanggal 5 Mei 2024 hingga 8 Mei 2024, FortifyTech melibatkan CyberShield untuk mengevaluasi posisi keamanan infrastrukturnya dibandingkan dengan praktik terbaik industri saat ini, termasuk uji penetrasi jaringan internal. Phases of penetration testing activities include the following:

- Planning – Tujuan pelanggan dikumpulkan, dan peraturan keterlibatan diperoleh.
- Discovery – Melakukan pemindaian dan enumerasi untuk mengidentifikasi kerentanan potensial, area lemah, dan eksploit.
- Attack – Konfirmasi kerentanan potensial melalui eksploitasi dan melakukan penemuan tambahan saat akses baru.
- Reporting – Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, percobaan yang gagal, dan kekuatan dan kelemahan perusahaan.



Assessment Components

Internal Pentration Test

Uji penetrasi internal adalah salah satu komponen penting dalam evaluasi keamanan yang bertujuan untuk mengidentifikasi kerentanan dan celah keamanan yang mungkin ada dalam jaringan internal perusahaan.

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	Temuan kritis menggambarkan kerentanan yang memiliki potensi dampak serius terhadap kerahasiaan, integritas, atau ketersediaan sistem. Eksploitasi kerentanan ini dapat mengakibatkan akses penuh ke sistem, kerugian data kritis, atau gangguan layanan yang signifikan.
High	7.0-8.9	Temuan tinggi menunjukkan kerentanan yang memiliki potensi dampak yang signifikan terhadap keamanan sistem. Meskipun tidak seberat temuan kritis, eksploitasi kerentanan ini masih dapat menghasilkan akses yang tidak sah atau pencurian data sensitif.
Moderate	4.0-6.9	Temuan menengah mencakup kerentanan yang memiliki potensi dampak moderat terhadap keamanan sistem. Meskipun mungkin tidak langsung mengancam kerahasiaan atau integritas data, eksploitasi kerentanan ini masih dapat menyebabkan gangguan operasional atau akses tidak sah ke sistem.
Low	0.1-3.9	Temuan rendah menunjukkan kerentanan yang memiliki dampak minimal terhadap keamanan sistem. Eksploitasi kerentanan ini mungkin memerlukan kondisi khusus atau akses yang terbatas, dan dampaknya terhadap operasional sistem terbatas.
Informational	N/A	Saran atau rekomendasi untuk peningkatan keamanan, tetapi tidak memerlukan tindakan perbaikan segera.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

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

Impact

Dampak mengukur dampak potensi kerentanan terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerusakan reputasi, dan kerugian finansial.

Scope

Assessment	Details
BlackBox Penetration Test	10.15.42.36
BlackBox Penetration Test	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 ITS Wifi/VPN

Executive Summary

TCMS evaluated Demo Corp's internal security posture through penetration testing from February 22nd, 2021 to March 5th, 2021. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten (10) business days.

Testing Summary

Pengujian dilakukan berdasarkan informasi awal yang diberikan, yaitu dua alamat IP yang dapat diakses, yaitu 10.15.42.36 dan 10.15.42.7. Saat mencoba membuka link pertama, 10.15.42.36, pada peramban, tidak ada yang ditampilkan. Oleh karena itu, pengujian dilanjutkan dengan menggunakan perangkat lunak nmap untuk memeriksa link tersebut.

Hasil pemindaian nmap memberikan informasi penting bahwa terdapat 3 port yang terbuka dengan jenis yang berbeda. Pengujian berhasil mengakses port 8888 pada peramban, dan ditemukan sebuah halaman login. Namun, tidak ditemukan informasi penting pada saat itu. Pengujian juga mencoba port lain yang terbuka, yaitu port 21 dengan jenis FTP. Di port ini, pengujian berhasil masuk ke FTP setelah beberapa percobaan, dan diketahui bahwa nama pengguna yang digunakan adalah umum dan terdapat kelemahan pada kata sandi yang digunakan. Jika seseorang mencoba masuk ke akun tanpa memasukkan kata sandi apa pun atau dengan kata sandi acak, sistem akan menganggapnya sebagai percobaan login yang berhasil.

Di port FTP tersebut, pengujian dapat mengakses file yang ada di dalamnya. Pengujian juga menemukan file bernama "backup.sql", yang merupakan hasil dari server SQL. Dalam percakapan pada sistem, terdapat percobaan login yang berhasil. Ketika file tersebut dibuka, terlihat bahwa ada percobaan login dengan nama pengguna "admin" dan kata sandi yang di-hash. Pengujian mencoba menggunakan alat john the ripper untuk memecahkan hash dari kata sandi tersebut, tetapi tidak berhasil. Namun, celah keamanan ini sangat rentan, dan jika diberi waktu lebih lama, penyerang dapat melakukan eksploitasi yang lebih serius.

Tester Notes and Recommendations

1. **Hasil Pemindaian Port**: Pemindaian awal menggunakan nmap mengungkapkan tiga port terbuka pada alamat IP target (10.15.42.36). Port 8888 dapat diakses melalui peramban web, menuju halaman login. Selain itu, port 21 diidentifikasi sebagai layanan FTP, memungkinkan akses ke file dalam server.
2. **Kerentanan Login**: Selama pengujian, ditemukan bahwa layanan FTP pada port 21 menunjukkan kerentanan yang signifikan. Nama pengguna default atau umum diterima tanpa memerlukan kata sandi. Bahkan upaya dengan kata sandi acak atau tidak ada dianggap sebagai login yang berhasil oleh sistem. Ini menimbulkan risiko keamanan yang serius karena pengguna yang tidak sah dapat mengakses file sensitif dan potensial meretas server.
3. **Analisis File**: Dalam server FTP, ditemukan sebuah file bernama "backup.sal", yang diduga berisi cadangan server SQL. Pemeriksaan file ini mengungkapkan percobaan login, termasuk salah satunya dengan nama pengguna "admin" dan kata sandi yang di-hash. Meskipun upaya untuk memecahkan kata sandi yang di-hash menggunakan alat seperti John the Ripper tidak berhasil, keberadaan informasi login sensitif menekankan pentingnya memperkuat langkah-langkah keamanan

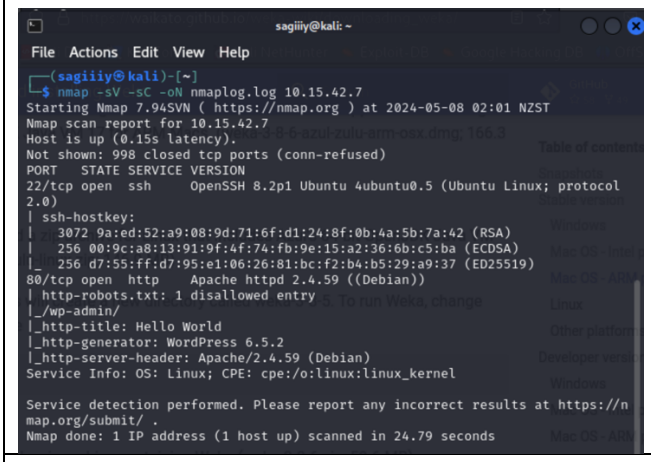
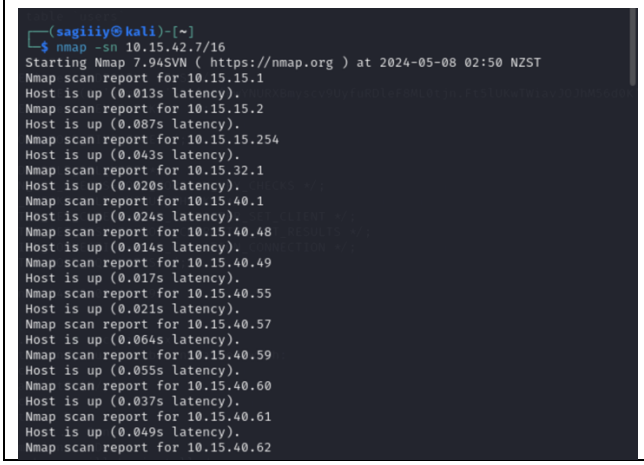
Reconnaissance and Digital Footprinting tools

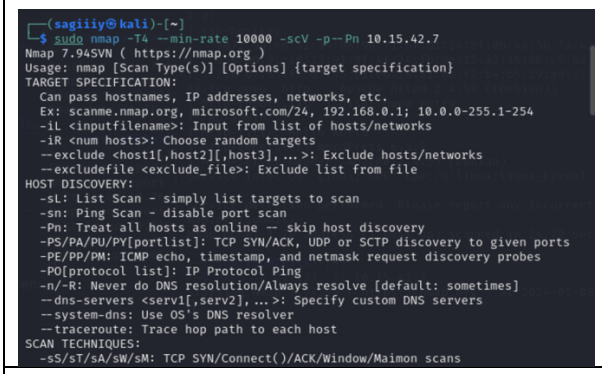
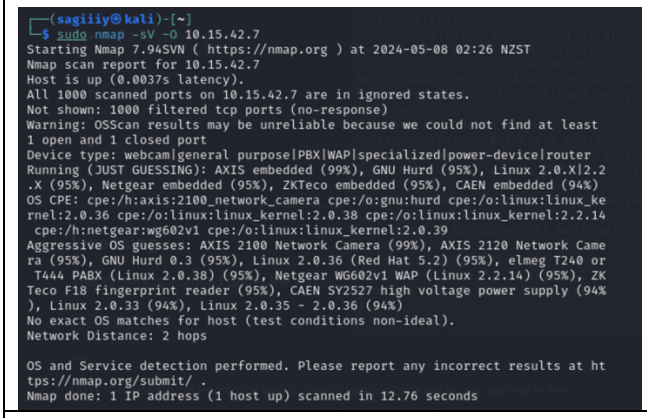
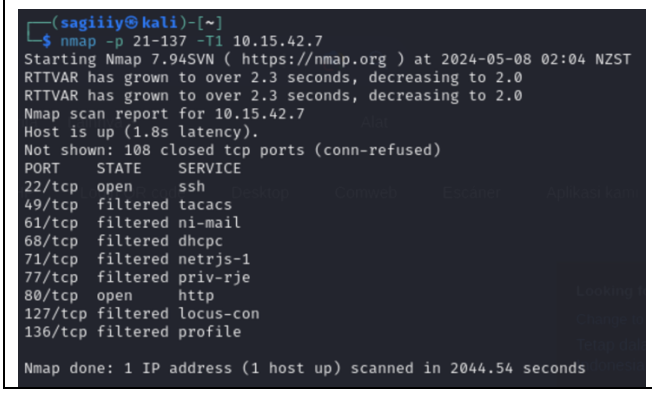
Peran yang sangat penting dalam pengujian keamanan dan aktivitas penelitian keamanan secara umum.

Nmap

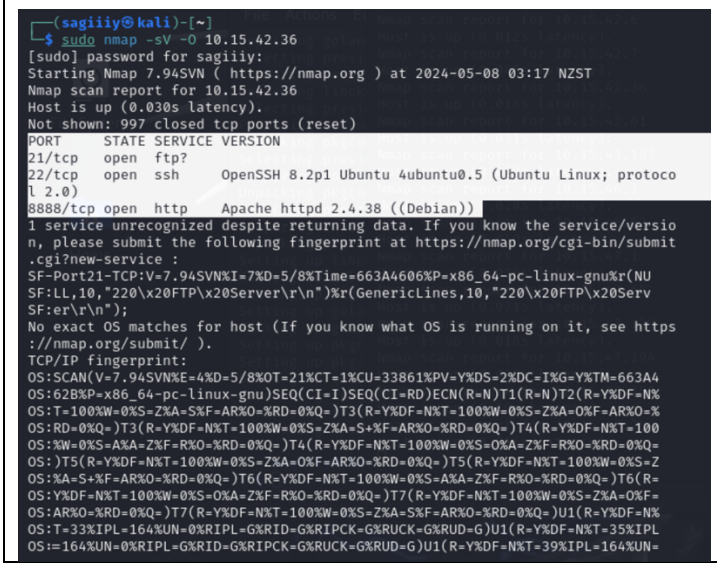
Sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal.

http:// http://10.15.42.7/

	**Nmap -sV -sC -oN nmaplog.log 10.15.42.7:** **untuk melakukan pemindaian jaringan terhadap host dengan alamat IP 10.15.42.7. Nmap akan mencoba mengidentifikasi versi perangkat lunak yang berjalan di port yang terbuka dan menjalankan serangkaian skrip skrip NSE yang dapat memberikan informasi tambahan tentang layanan yang berjalan.**
	**Nmap -sn 10.15.42.7/16:** **untuk melakukan pemindaian jaringan yang disebut "Ping Scan" terhadap rentang alamat IP tertentu.**

	Sudo nmap -T4 –min-rate 10000 -scV -p—Pn 10.15.42.7: perintah yang menggunakan utilitas Nmap untuk melakukan pemindaian jaringan terhadap host dengan alamat IP 10.15.42.7.
	Sudo nmap -sV -O 10.15.42.7: akan menjalankan Nmap dengan opsi untuk melakukan pemindaian port, mendeteksi versi layanan, dan mengidentifikasi sistem operasi dari perangkat yang memiliki alamat IP 10.15.42.7.
	Nmap -p 21-137 -T1 10.15.42.7: akan menjalankan Nmap dengan opsi untuk melakukan pemindaian pada rentang port yang ditentukan (dari port 21 hingga port 137) dengan kecepatan pemindaian yang rendah.

http:// http://10.15.42.36/

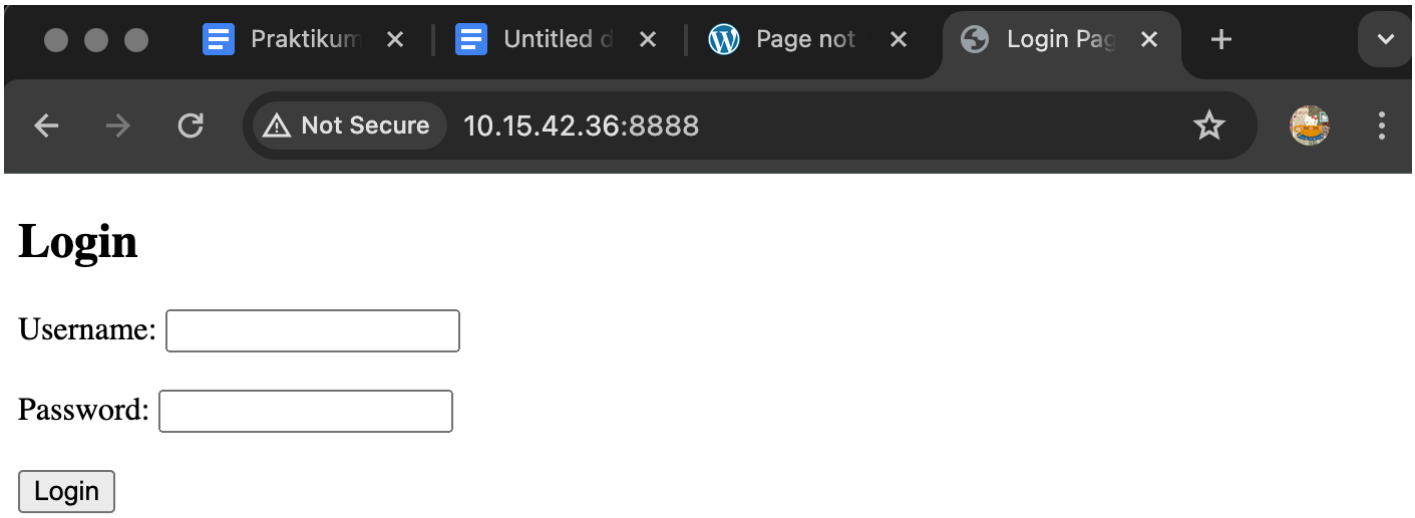


```
┌──(sagiiiy㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.36
[sudo] password for sagiiiy:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 03:17 NZST
Nmap scan report for 10.15.42.36
Host is up (0.030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=5/8%Time=663A4606%P=x86_64-pc-linux-gnu%r(NU
SF:LL,10,"220\x20FTP\x20Server\r\n")%r(GenericLines,10,"220\x20FTP\x20Serv
SF:er\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/8%OT=21%CT=1%CU=33861%PV=Y%DS=2%DC=I%G=Y%TM=663A4
OS:62B%P=x86_64-pc-linux-gnu)SEQ(CI=I)SEQ(CI=RD)ECN(R=N)T1(R=N)T2(R=Y%DF=N%
OS:T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=AR%O=%
OS:RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=100
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=O%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=
OS:Y%DF=N%T=100%W=0%S=O%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=
OS:AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=33%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=Y%DF=N%T=35%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=Y%DF=N%T=39%IPL=164%UN=
```

Sudo nmap -sV -O 10.15.42.36:

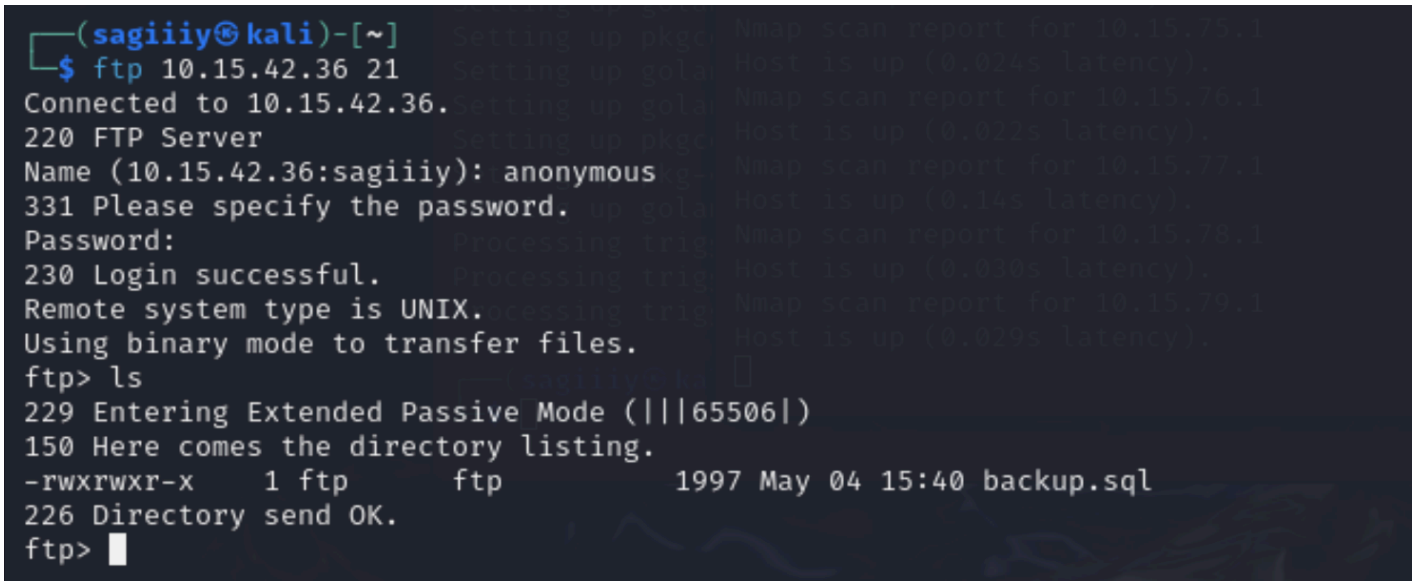
akan menjalankan Nmap dengan opsi untuk melakukan pemindaian port, mendeteksi versi layanan, dan mengidentifikasi sistem operasi dari perangkat yang memiliki alamat IP 10.15.42.36.

Hasil Sudo nmap -sV -O 10.15.42.36 ada open port 8888, saat di search di webstie 10.15.42.36:8888 akan muncul seperti berikut :

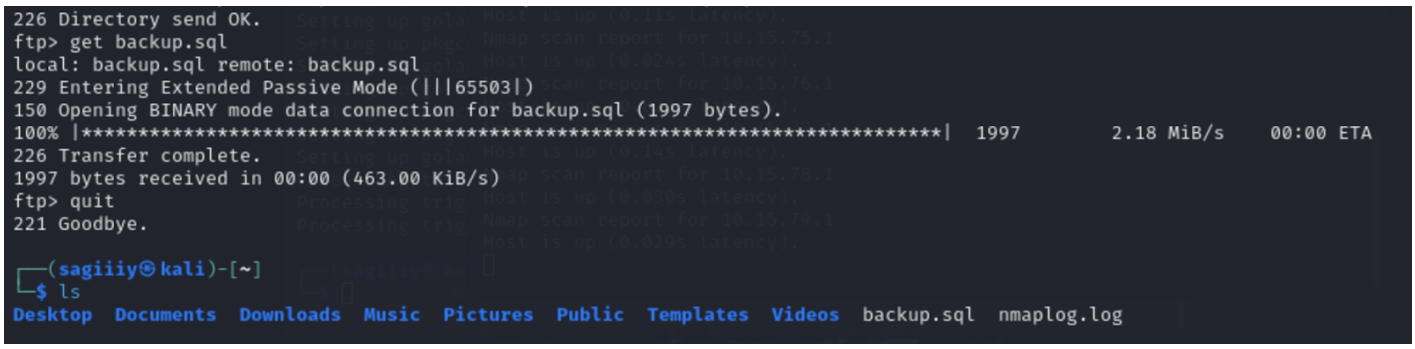


FTP

FTP (File Transfer Protocol) digunakan untuk mentransfer file antara komputer Anda dan server FTP yang ditentukan dengan alamat IP 10.15.42.36. Dengan menggunakan FTP, Anda dapat melakukan berbagai tindakan seperti mengunggah (upload) file dari komputer lokal ke server FTP, mengunduh (download) file dari server FTP ke komputer lokal, menghapus file dari server FTP, dan bahkan mengelola struktur direktori pada server
FTP.

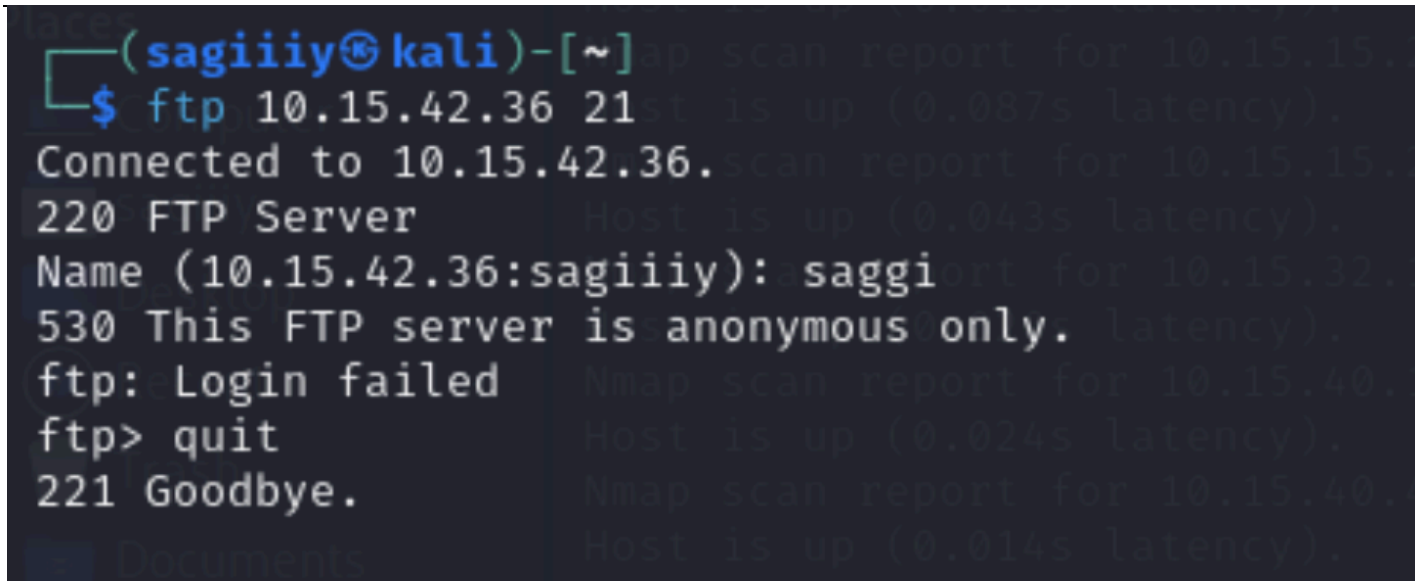


Dari ftp kita mendapat name = anonymous, Kemudian tanda 230 Login successful berarti berhasil



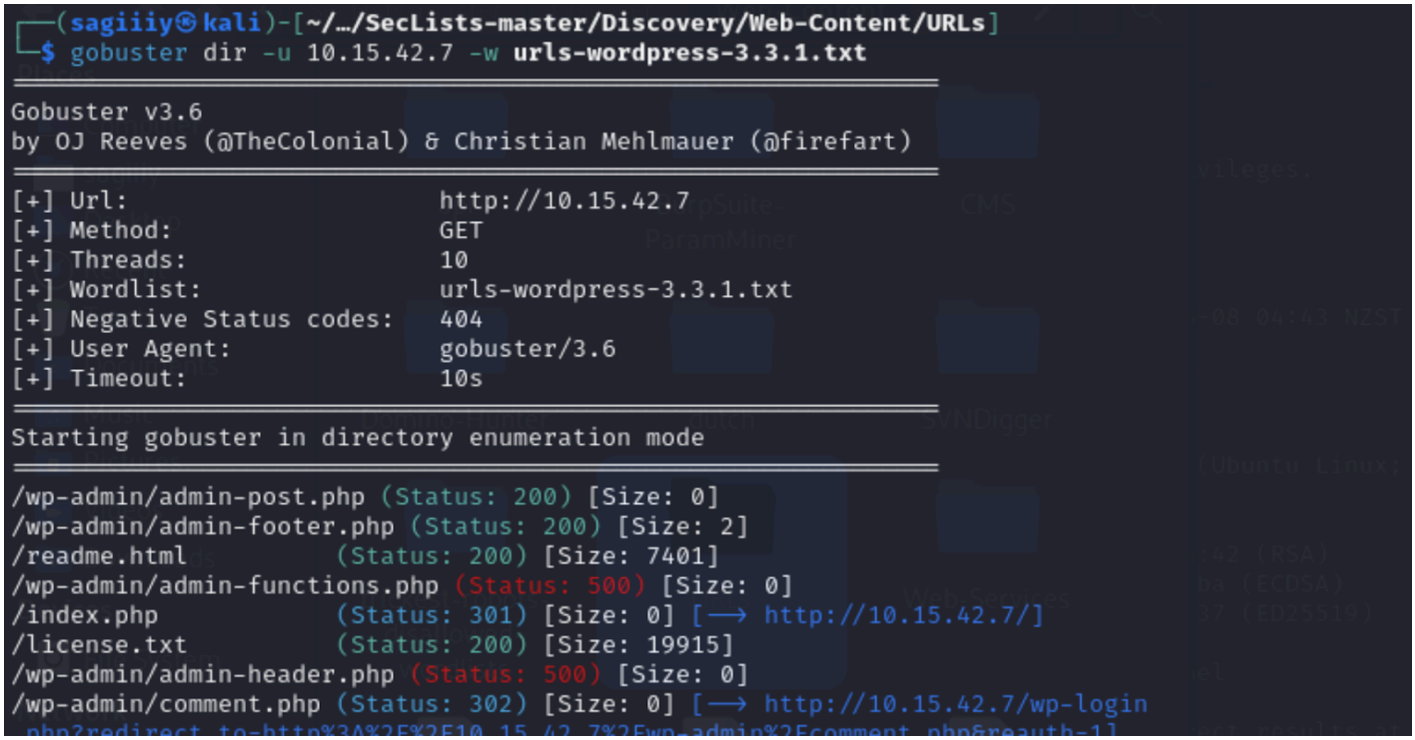
```
└─$ cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
-- ------------------------------------------------------
-- Server version       8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
```

```
DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2024-05-01 19:49:02

┌──(sagiiiy㉿kali)-[~]
└─$
```

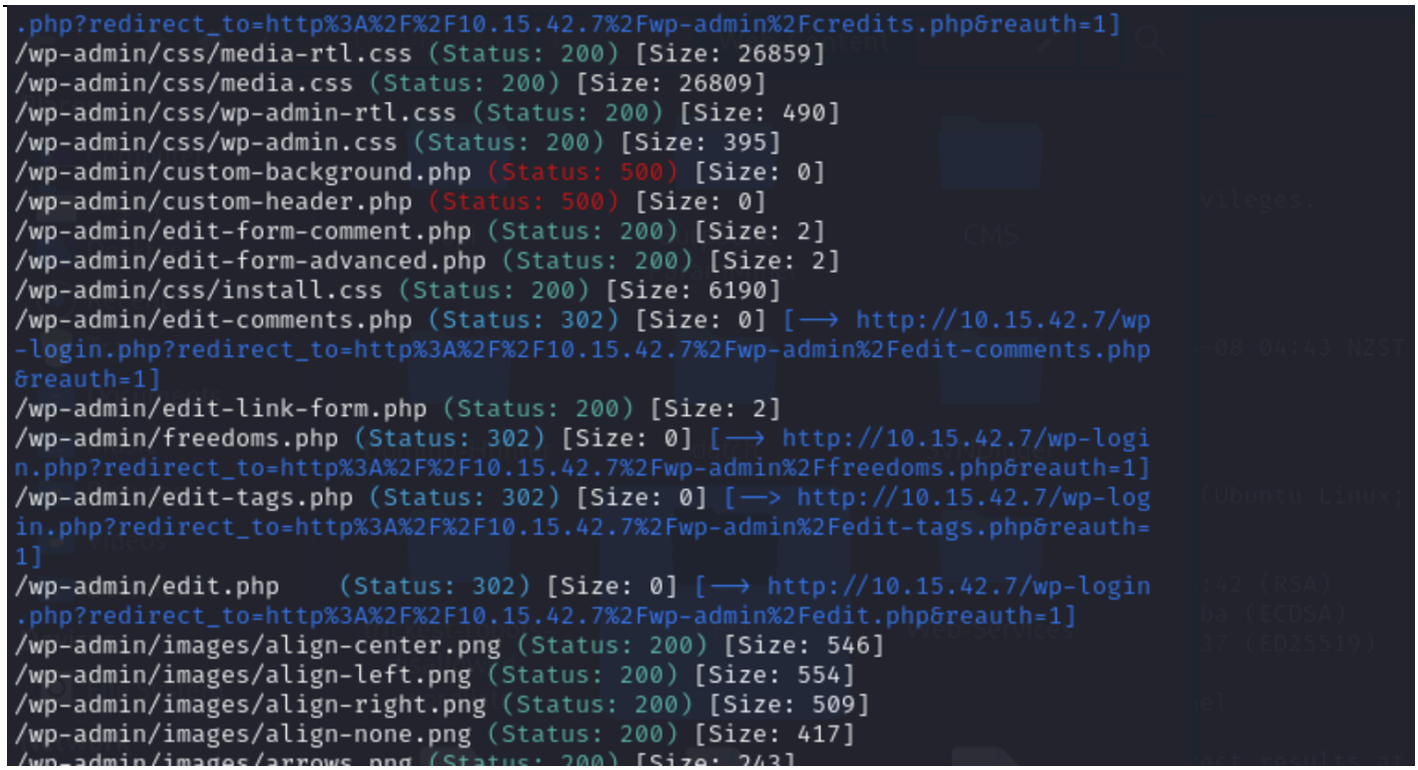


Gobuster

Gobuster merupakan tools yang berguna untuk scanning directory yang terdapat pada suatu web application. Menemukan directory pada suatu aplikasi web membuat tester memiliki jangkauan yang lebih luas untuk menganalisis kelemahan yang terdapat pada suatu web. Sederhananya, semakin besar fungsionalitas, semakin potensial sekumpulan developer melakukan kesalahan implementasi logic atau konfigutasi.



Hasil pemindaian menggunakan Gobuster versi 3.6 menunjukkan bahwa pemindaian dilakukan pada URL http://10.15.42.7 menggunakan metode GET dengan alat ParamMiner. Proses pemindaian dipercepat dengan penggunaan 10 thread yang bekerja secara simultan. Gobuster menggunakan daftar kata-kata dari file urls-wordpress-3.3.1.txt sebagai sumber untuk mencoba mengakses direktori atau berkas. Hanya kode status 404 yang dianggap negatif, sehingga jika Gobuster menemukan kode status 404 (Not Found), itu tidak akan dimasukkan dalam laporan pemindaian. Selain itu, Gobuster menggunakan string "gobuster/3.6" sebagai identifikasi agen pengguna dalam permintaan HTTP. Ini adalah ringkasan singkat dari konfigurasi dan parameter utama yang digunakan dalam pemindaian.

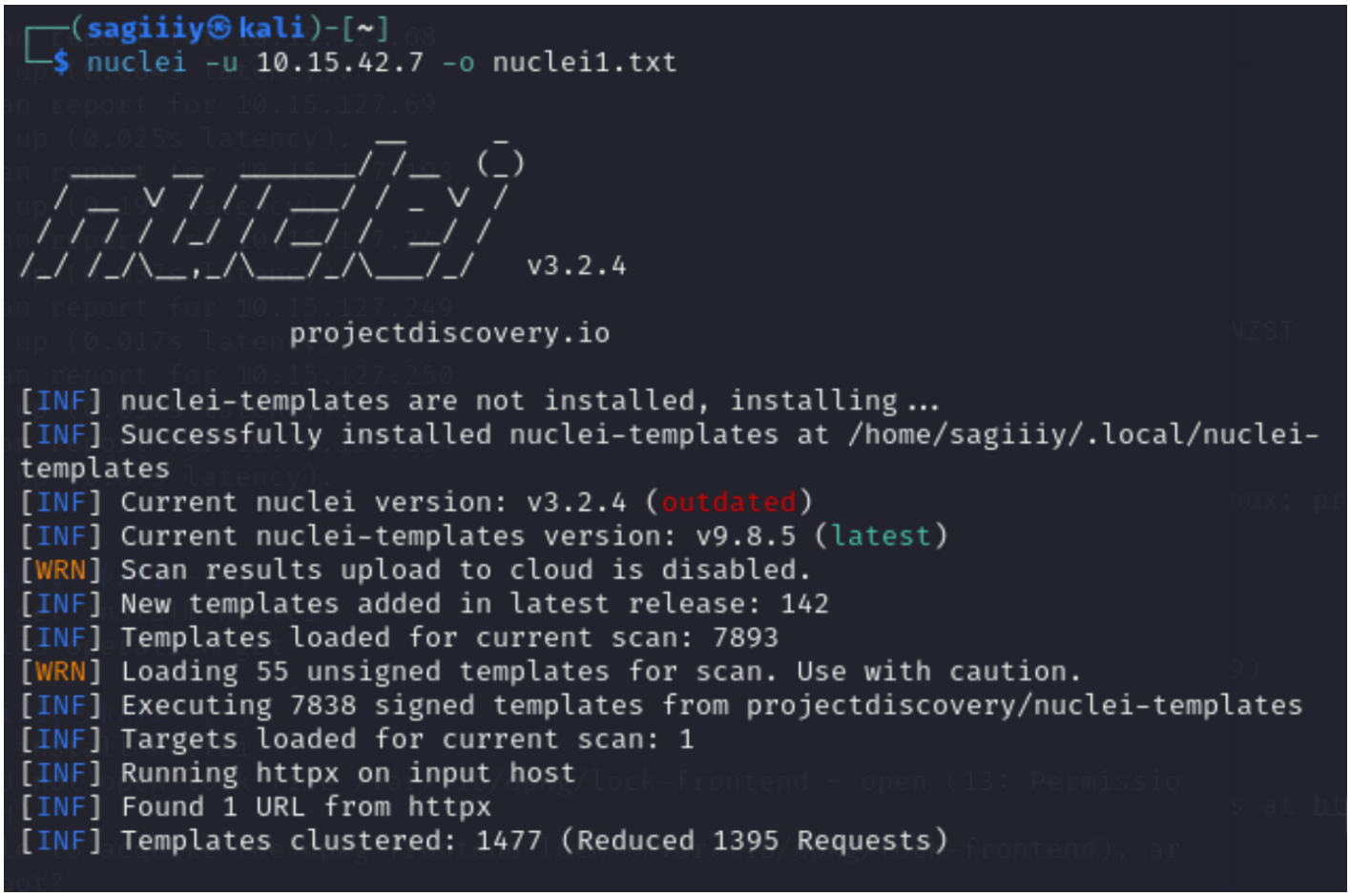


Vulnerability Scanning

Scanning atau yang sering disebut Vulnerability Assessment merupakan kegiatan yang dilakukan dalam penetration testing untuk melakukan identifikasi kerentanan pada suatu sistem secara otomatis dengan menggunakan tool atau software tambahan. sebuah alat open-source yang digunakan untuk melakukan pemindaian otomatis terhadap berbagai jenis kelemahan dan kerentanan pada aplikasi web dan infrastruktur.

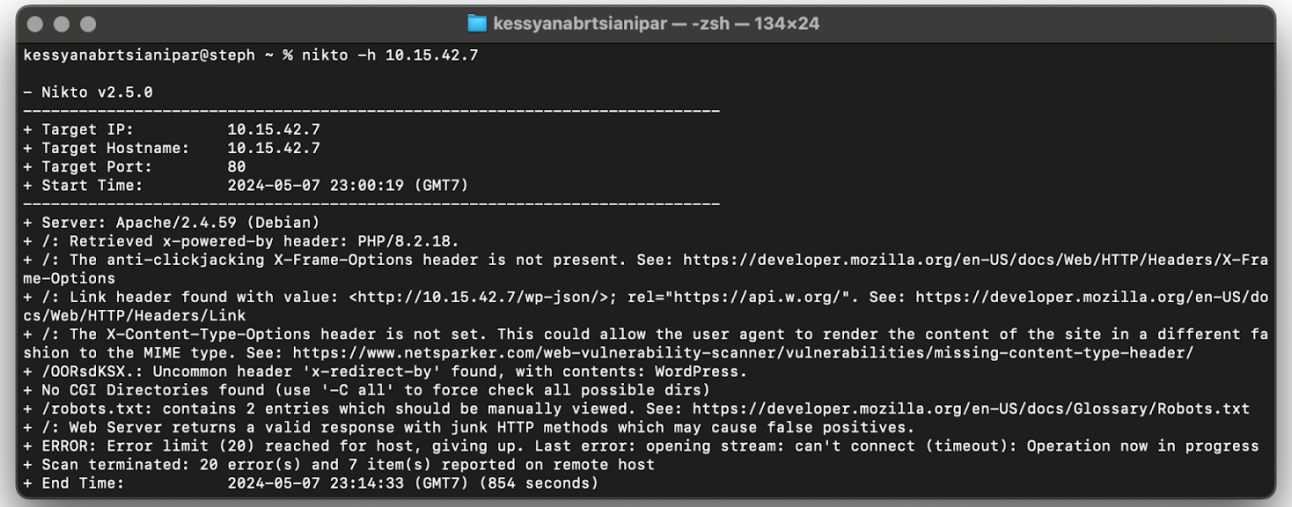
Nuclei

Sebuah alat open-source yang digunakan untuk melakukan pemindaian otomatis terhadap berbagai jenis kelemahan dan kerentanan pada aplikasi web dan infrastruktur.



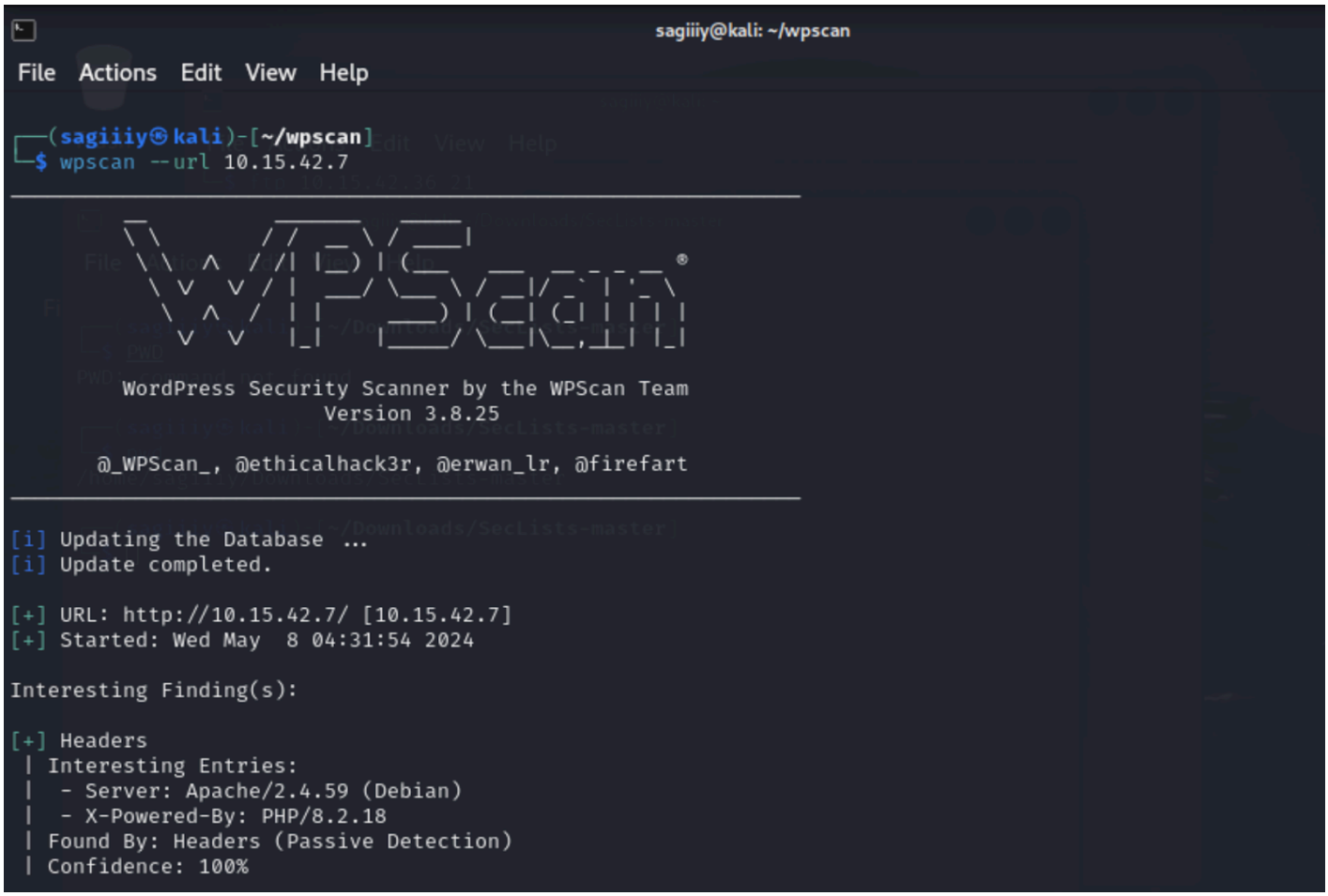
Nikto

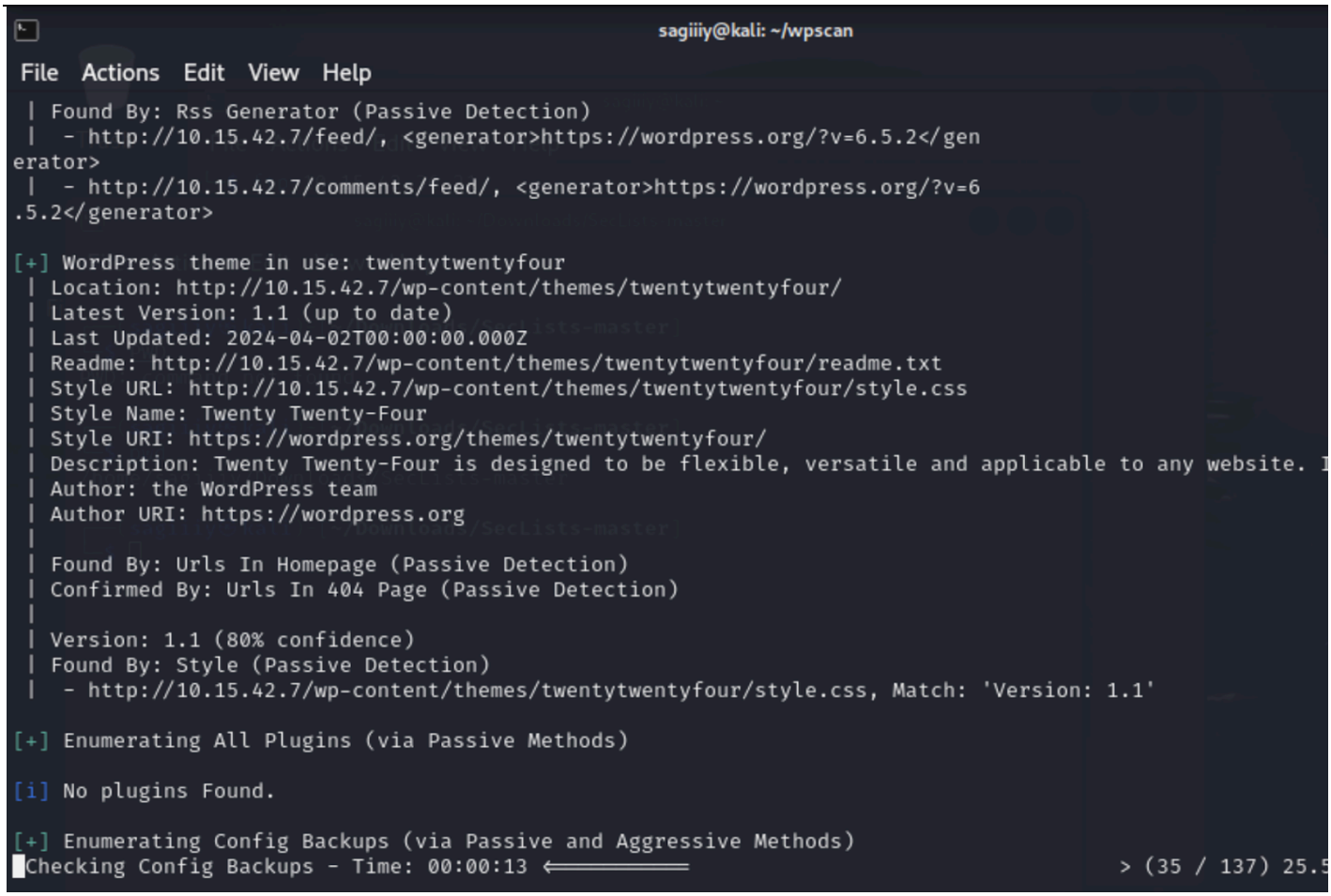
melakukan pemindaian secara otomatis terhadap situs web yang ditentukan dengan alamat IP 10.15.42.7 untuk mencari berbagai jenis kerentanan keamanan, termasuk serangan injeksi SQL, kerentanan XSS (Cross-Site Scripting), file yang dapat dieksekusi secara tidak aman, dan masih banyak
lagi.

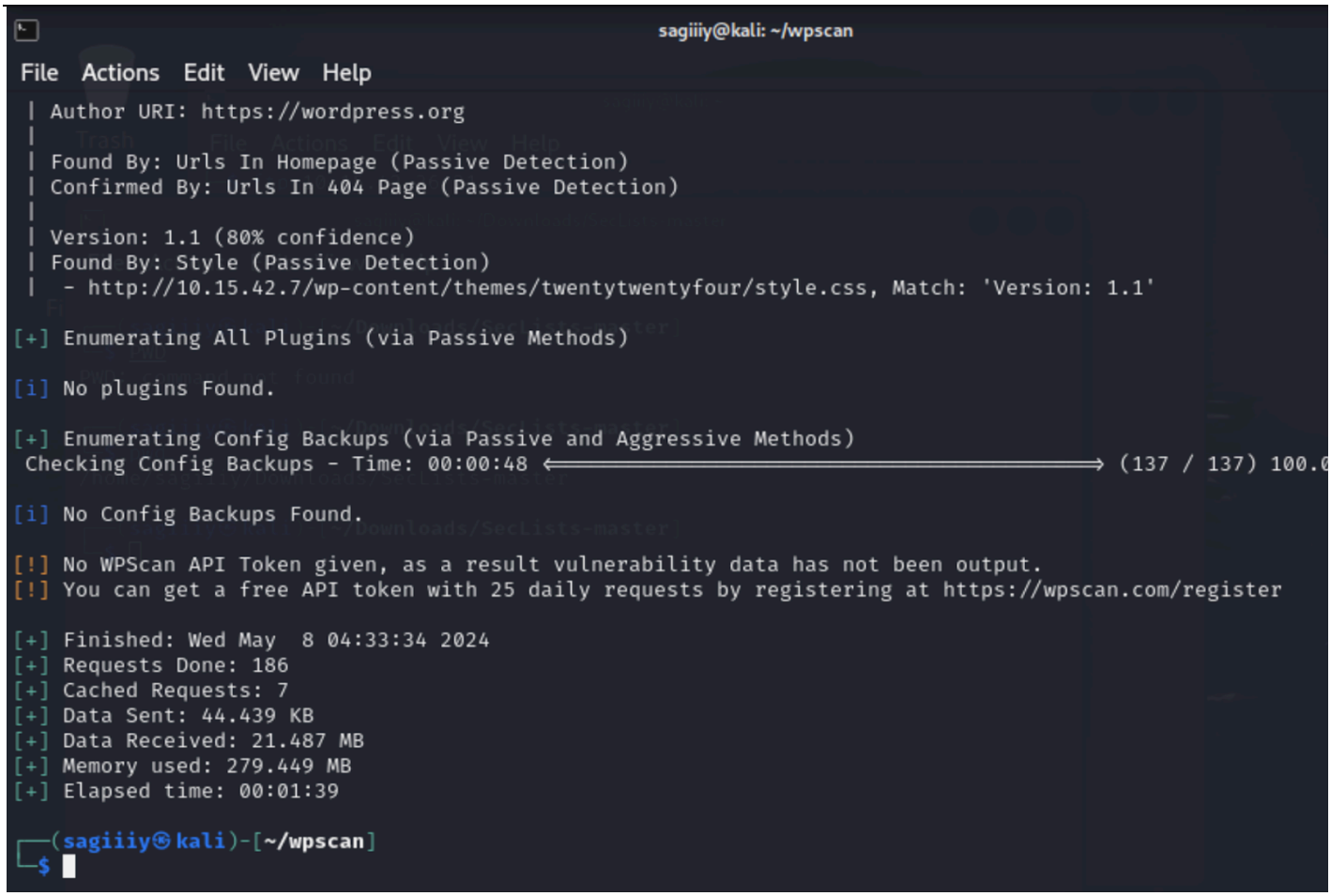


WPScan

Sebuah alat pemindaian keamanan yang khusus dirancang untuk WordPress. Alat ini memungkinkan pengguna untuk melakukan pemindaian otomatis terhadap situs web yang menggunakan platform WordPress, dengan tujuan mengidentifikasi kerentanan keamanan dan memperkuat keamanan situs tersebut.







Vulnerability Summary & Report Card

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

Blackbox Penetration Test Findings

0	2	1	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Blackbox Penetration Test		
BPT-001 : Port 21 ftp yang terbuka dengan akses yang mudah didapat	High	Memakai username dan password yang susah dan beragam
BPT-002 : File sql yang berisi username dan password dari admin	Moderate	Lakukan audit keamanan pada sistem untuk memastikan bahwa tidak ada lagi file-file berisi informasi sensitif
BPT-003 : File sql yang terekspos pada surface level security	Moderate	Memastikan untuk menutup akses publik terhadap file-file ini agar tidak dapat diakses oleh pihak yang tidak berwenang.
BPT-004 : Penemuan Port yang terbuka	Infromational	Memperhatikan port yang open dan close

Technical Findings

Blackbox Penetration Test Findings

BPT-001 : Port 21 ftp yang terbuka dengan akses yang mudah didapat

Description:	Setelah menemukan port yang terbuka di link pertama, yaitu 10.15.42.36, penguji dapat dengan cepat mengakses port-port tersebut, salah satunya adalah port 21 yang digunakan untuk FTP. Di port tersebut, proses login diperlukan dan penguji berhasil masuk dengan menebak username yang umum digunakan. Salah satu kerentanan lainnya adalah kurangnya validasi pada input password, sehingga jika kolom tersebut kosong atau diisi dengan kata apa pun, sistem akan tetap memberikan pesan "Login Successful"
Risk:	Dengan memanfaatkan kerentanan ini, penyerang dapat dengan mudah mendapatkan akses yang tidak sah ke dalam sistem atau server.
System:	All
Tools Used:	Ftp
References:	https://www.ibm.com/docs/fr/i/7.2?topic=i-ftp-reference-information

Evidence

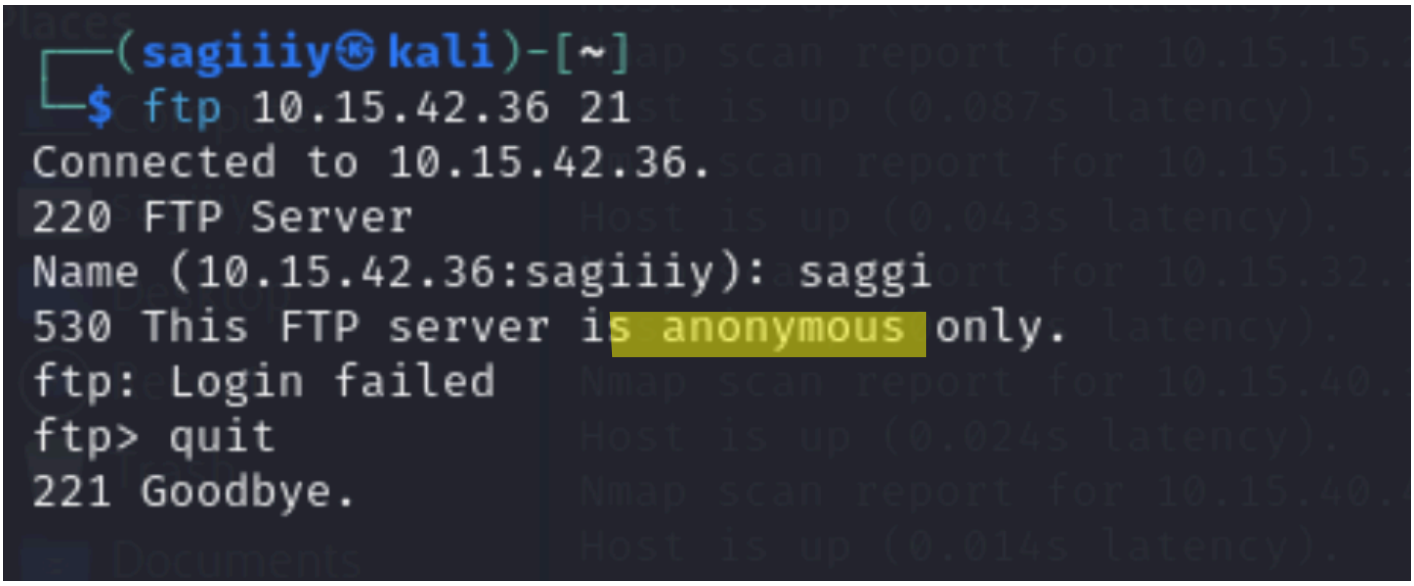


Figure 1: Saat salah masukin name ada tulsisan anonymous

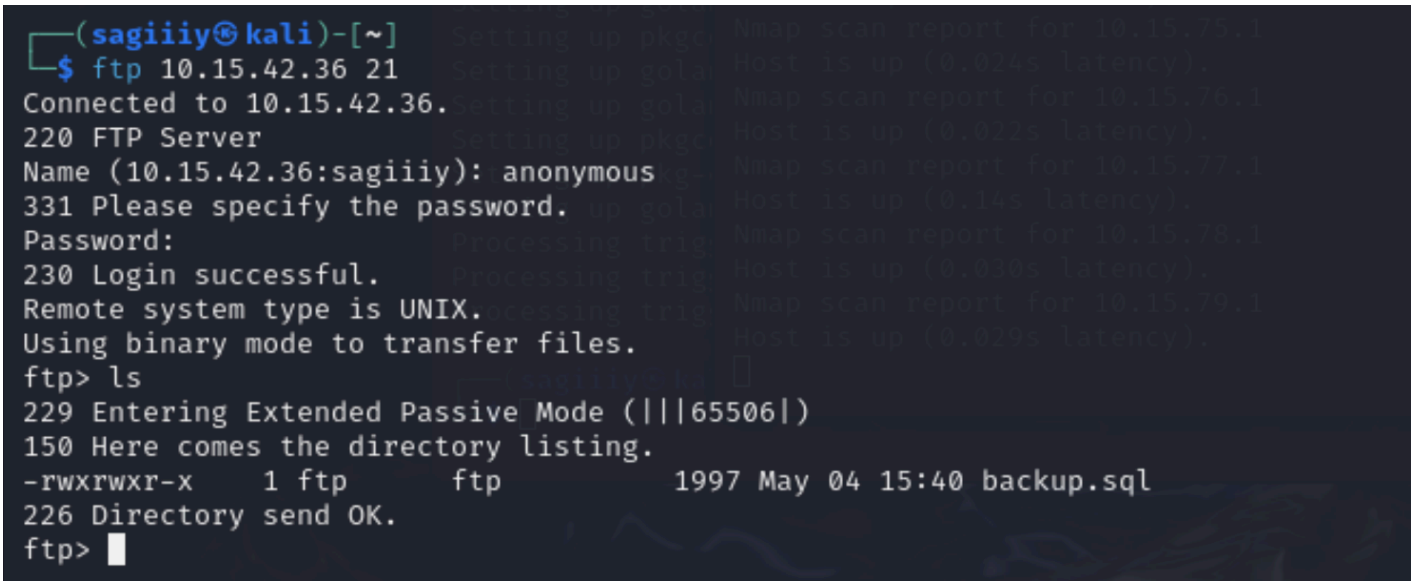


Figure 2 : Saat kita masukin anonymous bisa

Finding BPT-002: File sql yang berisi username dan password dari admin

Description:	File yang sebelumnya dapat diakses dan diunduh, yaitu "backup.sql", telah diproses dan kontennya dianalisis. Dalam file tersebut, teridentifikasi bahwa telah dilakukan percobaan login yang sukses dengan menggunakan nama pengguna "admin" dan kata sandi yang telah di-hash.
Risk:	Dengan mengetahui bahwa akun "admin" dapat digunakan untuk login, penyerang dapat mencoba masuk ke dalam sistem dengan menggunakan kredensial yang telah ditemukan. Ini bisa mengakibatkan akses yang tidak sah ke hak istimewa administrator, memberikan kontrol penuh atas sistem.
System:	All
Tools Used:	Hashmap
References:	https://www.interviewcake.com/concept/java/hash-map

Evidence

```
└─$ cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
-- ------------------------------------------------------
-- Server version       8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--


DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2024-05-01 19:49:02

┌──(sagiiiy㉿kali)-[~]
└─$
```

Figure 3: cat backup.sql

Finding BPT-003: File sql yang terekspos pada surface level security

Description:	Di link yang sama, 10.15.42.36, pada port 21 yang berhasil diakses dengan login, terdapat satu file yang terlihat secara langsung yaitu "backup.sql". File tersebut dapat ditemukan dengan perintah "get backup.sql" langsung setelah berhasil login.
Risk:	Jika file "backup.sql" mengandung informasi sensitif seperti kredensial pengguna, data pelanggan, atau data bisnis penting lainnya, akses tidak sah ke file tersebut dapat mengakibatkan pencurian informasi sensitif.
System:	All
Tools Used:	nmap
References:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/

Evidence

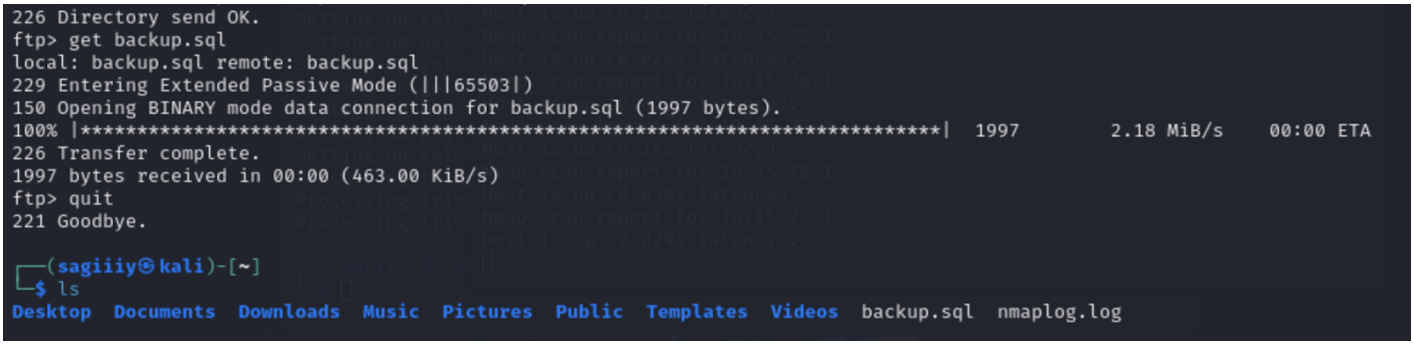


Figure 4: Get backup.sql

Finding BPT-004: Penemuan Port yang terbuka

Description:	Memberikan informasi terperinci tentang port yang terbuka, termasuk nomor portnya dan layanan yang berjalan di dalamnya, serta versi perangkat lunak yang terdeteksi. Selain itu, deskripsi juga mungkin mencakup perkiraan sistem operasi target berdasarkan karakteristik jaringan yang teramati oleh nmap.
Risk:	Port terbuka dapat menjadi titik masuk potensial bagi penyerang dari luar untuk mencoba mengeksploitasi sistem
System:	All
Tools Used:	nmap
References:	https://phoenixnap.com/kb/nmap-scan-open-ports

Evidence

```
┌──(sagiiiy㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.36
[sudo] password for sagiiiy:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 03:17 NZST
Nmap scan report for 10.15.42.36
Host is up (0.030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=5/8%Time=663A4606%P=x86_64-pc-linux-gnu%r(NU
SF:LL,10,"220\x20FTP\x20Server\r\n")%r(GenericLines,10,"220\x20FTP\x20Serv
SF:er\r\n");
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=5/8%OT=21%CT=1%CU=33861%PV=Y%DS=2%DC=I%G=Y%TM=663A4
OS:62B%P=x86_64-pc-linux-gnu)SEQ(CI=I)SEQ(CI=RD)ECN(R=N)T1(R=N)T2(R=Y%DF=N%
OS:T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=AR%O=%
OS:RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=100
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=O%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=
OS:Y%DF=N%T=100%W=0%S=O%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=O%F=
OS:AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=33%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=Y%DF=N%T=35%IPL
OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=Y%DF=N%T=39%IPL=164%UN=
```

Figure 5: Penempuan port yang terbuka

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

Last Page