



FortifyTech

Security Assessment Findings Report

Muhammad Rifqi Oktaviansyah - 5027221067

Date: May 8, 2024

SCOPE

Assesment	Details
Internal Penetration Test	10.15.42.36
	10.15.42.7

Client Allowances

- Pengerjaan hanya bisa menggunakan jaringan ITS (wifi ITS / vpn ITS)
- Dilarang melakukan hal-hal yang diluar etika

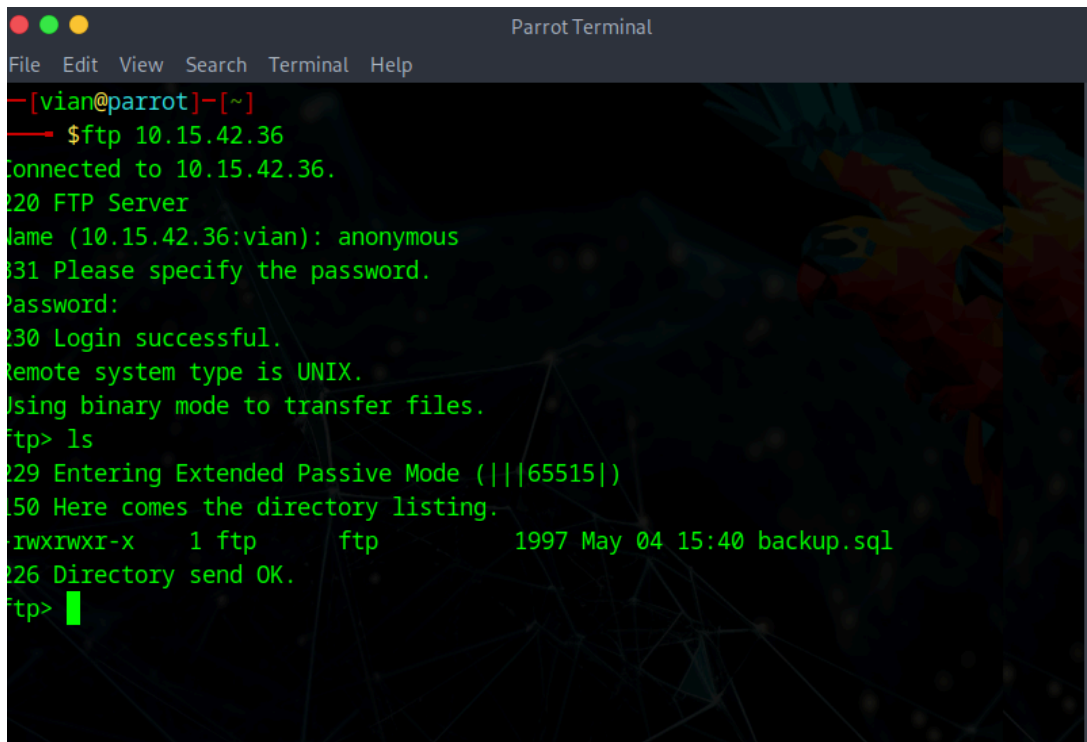
SUMMARY

- Scoping atau pentesting dilakukan mulai dari tanggal 5 Mei 2024 hingga 8 Mei 2024.
- Beberapa tools yang digunakan dalam reconnaissance antara lain nmap dan dirb
- Sedangkan tools yang digunakan dalam vulnerability analysis adalah website cve dan berbagai sumber dari internet
- Pada IP **10.15.42.36** ditemukan 3 port yaitu: 21, 22, dan 8888
- Port 21 merupakan FTP service yang menggunakan versi vsftpd 2.0.8 or later. Lalu ditemukan juga kalau FTP tersebut memperbolehkan Anonymous login dengan kode FTP 230. Untuk login ftp hanya memerlukan username anonymous dan tidak perlu memasukkan password. Hal ini tentunya sangat rentan akan pembobolan oleh pihak yang tidak bertanggung jawab. Didalam FTP terdapat satu file dump bernama backup.sql. Pada FTP kita hanya memiliki permission untuk membuka dan mengunduh file saja.
- Port 22 merupakan SSH service yang menggunakan versi OpenSSH 8.2p1 Ubuntu 4ubuntu0.5. Versi tersebut memiliki kerentanan kritis seperti yang tertera pada dokumentasi **CVE-2023-38408**. Kerentanan tersebut dapat di patch atau diperbaiki dengan menggunakan versi open ssh yang terbaru.
- Port 8888 merupakan web login page html sederhana yang menggunakan versi Apache 2.4.38. dan sistem operasi Linux Debian. Apache 2.4.38 memiliki kerentanan exploit tinggi seperti yang tertera pada dokumentasi **CVE-2019-021**. Exploit ini dapat dicegah dengan menggunakan versi Apache yang terbaru.
- Pada IP **10.15.42.7** ditemukan 2 port yaitu: 22 dan 80.
- Port 22 merupakan SSH service yang menggunakan versi yang sama dengan IP 10.15.42.36 yaitu OpenSSH 8.2p1 Ubuntu 4ubuntu0.5. Dengan exploit yang sama juga.
- Port 80 merupakan web yang berbasis versi Apache 2.4.59 dan Wordpress 6.5.2.

Technical Findings

Description:	Pada FTP port 21 dapat dibuka dengan cara memasukkan username anonymous dan klik enter tanpa harus mengisi saat memasukkan password.
Impact:	Low
System:	10.15.42.36
References:	https://www.ninjaone.com/it-hub/end-point-security/what-is-ftp-anonymous-login/

Evidence:



```
Parrot Terminal
File Edit View Search Terminal Help
~[vian@parrot]-[~]
$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:vian): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (||65515|)
150 Here comes the directory listing.
-rwxrwxr-x  1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> █
```

1.0. Login FTP

```

GNU nano 7.2                                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 */;

```

1.1 Isi file backup.sql 1

```

GNU nano 7.2                                backup.sql
) 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.Ft5lUKwTWiavJ0JhM56d0K');
/*!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

```

1.2. Isi file backup.sql 2