



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.

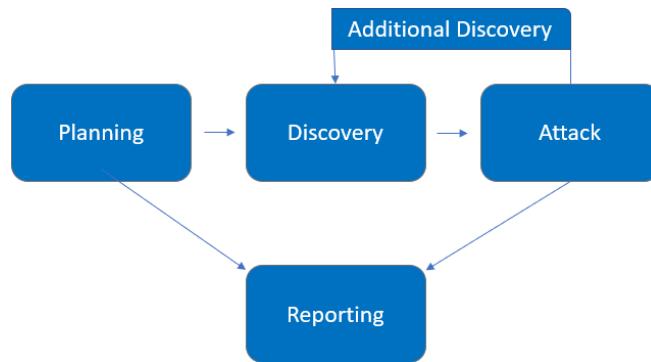
Contact Information

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 eksloit.
- Attack – Konfirmasi kerentanan potensial melalui eksloitasi dan melakukan penemuan tambahan saat akses baru.
- Reporting – Mendokumentasikan semua kerentanan dan eksloitasi yang ditemukan, percobaan yang gagal, dan kekuatan dan kelemahan perusahaan.



Assessment Components

Internal Penetration 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. Eksloitasi 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, eksloitasi 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, eksloitasi 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. Eksloitasi 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 dieksloitasi. 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 eksloitasi 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://10.15.42.7>

```
(sagiiy㉿kali)-[~]
$ nmap -sV -sC -oN nmaplog.log 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:01 NZST
Nmap scan report for 10.15.42.7
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 9a:ed:52:a9:08:9d:71:f6:df:12:24:8f:0b:4a:5b:7a:42 (RSA)
|_ 256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_ 256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp    open  http    Apache httpd 2.4.59 (Debian)
| http-robots.txt: 1 disallowed entry. To run Weka, change
|_ /wp-admin/
|_ http-title: Hello World
|_ http-generator: WordPress 6.5.2
|_ http-server-header: Apache/2.4.59 (Debian)
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 24.79 seconds
```

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.

```
(sagiiy㉿kali)-[~]
$ nmap -sn 10.15.42.7/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:50 NZST
Nmap scan report for 10.15.42.1
Host is up (0.013s latency).
Nmap scan report for 10.15.42.2
Host is up (0.087s latency).
Nmap scan report for 10.15.42.254
Host is up (0.043s latency).
Nmap scan report for 10.15.32.1
Host is up (0.020s latency).
Nmap scan report for 10.15.40.1
Host is up (0.024s latency).
Nmap scan report for 10.15.40.48
Host is up (0.014s latency).
Nmap scan report for 10.15.40.49
Host is up (0.017s latency).
Nmap scan report for 10.15.40.55
Host is up (0.021s latency).
Nmap scan report for 10.15.40.57
Host is up (0.064s latency).
Nmap scan report for 10.15.40.59
Host is up (0.055s latency).
Nmap scan report for 10.15.40.60
Host is up (0.037s latency).
Nmap scan report for 10.15.40.61
Host is up (0.049s latency).
Nmap scan report for 10.15.40.62
```

Nmap -sn 10.15.42.7/16:
untuk melakukan pemindaian jaringan yang disebut "Ping Scan" terhadap rentang alamat IP tertentu.

```
(sagiiiy㉿kali)-[~]
└─$ sudo nmap -T4 --min-rate 10000 -scV -p--Prn 10.15.42.7
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>; Input from list of hosts/networks
  -iR <num hosts>; Choose random targets
  --exclude <host1[,host2][,host3], ...>; Exclude hosts/networks
  --excludedfile <exclude_file>; Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PV/PV[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  -dns-servers <serv1[,serv2], ...>; Specify custom DNS servers
  -system-dns: Use OS's DNS resolver
  -traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-sT/-sW/-sM: TCP SYN/Connect()//ACK/Window/Maimon scans
```

Sudo nmap -T4 --min-rate 10000 -scV -p--Prn 10.15.42.7:

perintah yang menggunakan utilitas Nmap untuk melakukan pemindaian jaringan terhadap host dengan alamat IP 10.15.42.7.

```
(sagiiiy㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:26 NZST
Nmap scan report for 10.15.42.7
Host is up (0.0037s latency).
All 1000 scanned ports on 10.15.42.7 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: webcam|general purpose|PBX|WAP|specialized|power-device|router
Running (JUST GUESSING): AXIS embedded (99%), GNU Hurd (95%), Linux 2.0.X|2.2.X (95%), Netgear embedded (95%), ZKTeco embedded (95%), CAEN embedded (94%)
OS CPE: cpe:/h:axis:2100_network_camera cpe:/o:gnu:hurd cpe:/o:linux:linux_kernel:2.0.38 cpe:/o:linux:linux_kernel:2.2.14 cpe:/h:netgear:wg602v1 cpe:/o:linux:linux_kernel:2.0.39
Aggressive OS guesses: AXIS 2100 Network Camera (99%), AXIS 2120 Network Camera (95%), GNU Hurd 0.3 (95%), Linux 2.0.36 (Red Hat 5.2) (95%), elmeg T240 or T444 PABX (Linux 2.0.38) (95%), Netgear WG602v1 WAP (Linux 2.2.14) (95%), ZKTeco F18 fingerprint reader (95%), CAEN SY2527 high voltage power supply (94%), Linux 2.0.33 (94%), Linux 2.0.35 - 2.0.36 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds
```

Sudo nmap -sV -O 10.15.42.7:

akan menjalankan Nmap dengan opsi untuk melakukan pemindaian port, mendekripsi versi layanan, dan mengidentifikasi sistem operasi dari perangkat yang memiliki alamat IP 10.15.42.7.

```
(sagiiiy㉿kali)-[~]
└─$ nmap -p 21-137 -T1 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 02:04 NZST
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.15.42.7
Host is up (1.8s latency).
Not shown: 108 closed tcp ports (conn-refused)
PORT      STATE     SERVICE
22/tcp    open      ssh      Desktop      Comweb      Scanner      Aplikasi kant
49/tcp    filtered tacacs
61/tcp    filtered ni-mail
68/tcp    filtered dhcpc
71/tcp    filtered netrjs-1
77/tcp    filtered priv-rje
80/tcp    open      http
127/tcp   filtered locus-con
136/tcp   filtered profile

Nmap done: 1 IP address (1 host up) scanned in 2044.54 seconds
```

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.

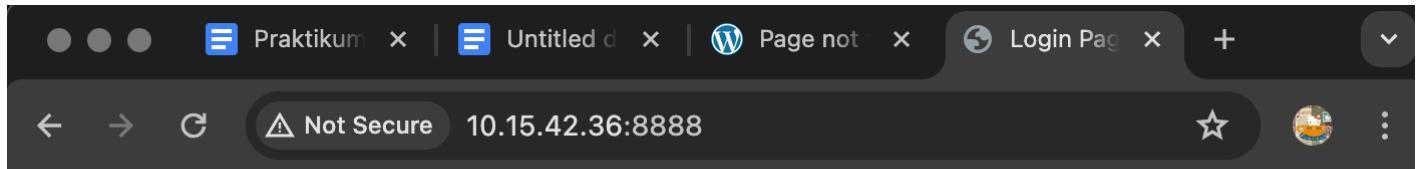
http:// http://10.15.42.36/

```
[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).
Nmap scan report for 10.15.42.36
Host is up (0.030s latency).
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  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 to https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=5/8%OT=21%CT=1%CU=33861%PV=Y%DS=2%DC=I%G=Y%TM=663A4
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%I=4%D=5/8%OT=21%CT=1%CU=33861%PV=Y%DS=2%DC=I%G=Y%TM=663A4
OS:628%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=0%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=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=100%W=0%S=0%A=Z%F=AR%O=%RD=0%Q=)
OS:T5(R=Y%DF=N%T=100%W=0%S=Z%A=0%F=AR%O+=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z%
OS:%A=5%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=AR%O=%RD=0%Q=)T6(R=
OS:Y%DF=N%T=100%W=0%S=0%A=Z%F=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%S=Z%A=0%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%T=35%IPL
OS:=133%IPL=164%UN=0%IPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=Y%DF=N%T=39%IPL=164%UN=
OS:=164%UN=0%IPL=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 :



Login

Username:

Password:

Login

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.

```
(sagiiiy㉿kali)-[~] Setting up pkgs Nmap scan report for 10.15.75.1
└─$ ftp 10.15.42.36 21 Setting up golang Host is up (0.024s latency).
Connected to 10.15.42.36. Setting up golang Nmap scan report for 10.15.76.1
220 FTP Server Setting up pkgs Host is up (0.022s latency).
Name (10.15.42.36:sagiiiy): anonymous Nmap scan report for 10.15.77.1
331 Please specify the password. up golang Host is up (0.14s latency).
Password: Processing trigger Nmap scan report for 10.15.78.1
230 Login successful. Processing trigger Host is up (0.030s latency).
Remote system type is UNIX. Processing trigger Nmap scan report for 10.15.79.1
Using binary mode to transfer files. Host is up (0.029s latency).
ftp> ls sagiiiy@kali: []
229 Entering Extended Passive Mode (|||65506|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May  4 15:40 backup.sql
226 Directory send OK.
ftp> █
```

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

```
226 Directory send OK. Setting up golang Host is up (0.11s latency).
ftp> get backup.sql Setting up pkgs Nmap scan report for 10.15.75.1
local: backup.sql remote: backup.sql Host is up (0.024s latency).
229 Entering Extended Passive Mode (|||65503|) scan report for 10.15.76.1
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% [*****] 1997 2.18 MiB/s 00:00 ETA
226 Transfer complete. Setting up golang Host is up (0.14s latency).
1997 bytes received in 00:00 (463.00 KiB/s) Nmap scan report for 10.15.78.1
ftp> quit Processing trigger Host is up (0.030s latency).
221 Goodbye. Processing trigger Nmap scan report for 10.15.79.1
Host is up (0.029s latency).
(sagiiiy㉿kali)-[~] ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  backup.sql  nmaplog.log
```

```

└─$ cat backup.sql
-- MySQL dump 10.13 Distrib 8.0.36, for Linux (x86_64) (for 10.15.81.1)
-- 
-- Host: localhost      Database: db
-- 
-- Server version     8.0.36-0ubuntu0.22.04.1
-- 
/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */; 13.84.1
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */; 
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */; 13.85.1
/*!50503 SET NAMES utf8mb4 */; 13.86.1
/*!40103 SET @OLD_TIME_ZONE=@TIME_ZONE */; 13.86.1
/*!40103 SET TIME_ZONE='+00:00' */; 13.86.1
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */; 13.87.107
/*!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 */; 13.88.1
-- 
-- Table structure for table `users` 
-- 
DROP TABLE IF EXISTS `users`; 13.89.1
/*!40101 SET @saved_cs_client      = @@character_set_client */; 13.90.1
/*!50503 SET character_set_client = utf8mb4 */; 13.91.1
CREATE TABLE `users` ( 13.92.1
    `id` int NOT NULL, 13.93.1
    `username` varchar(255) DEFAULT NULL, 13.94.1
    `password` varchar(255) DEFAULT NULL, 13.95.1
    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`; 13.81.1
/*!40101 SET @saved_cs_client      = @@character_set_client */; 13.82.1
/*!50503 SET character_set_client = utf8mb4 */; 13.83.1
CREATE TABLE `users` ( 13.84.1
    `id` int NOT NULL, 13.85.1
    `username` varchar(255) DEFAULT NULL, 13.86.1
    `password` varchar(255) DEFAULT NULL, 13.87.1
    PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci; 13.88.1
/*!40101 SET character_set_client = @saved_cs_client */; 13.89.1
-- 
-- Dumping data for table `users` 
-- 
LOCK TABLES `users` WRITE; 13.90.1
/*!40000 ALTER TABLE `users` DISABLE KEYS */; 13.91.1
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJ0JhM56d0K'); 13.92.1
/*!40000 ALTER TABLE `users` ENABLE KEYS */; 13.93.1
UNLOCK TABLES; 13.94.1
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */; 13.95.1
-- 
-- Dump completed on 2024-05-01 19:49:02

```

```
(sagiiiy㉿kali)-[~] ap scan report for 10.15.15.1
$ ftp 10.15.42.36 21st is up (0.087s latency).
Connected to 10.15.42.36.scan report for 10.15.15.1
220 FTP Server      Host is up (0.043s latency).
Name (10.15.42.36:sagiiiy):asaggiort for 10.15.32.
530 This FTP server is an anonymous@only. latency).
ftp: Login failed      Nmap scan report for 10.15.40.
ftp> quit              Host is up (0.024s latency).
221 Goodbye.           Nmap scan report for 10.15.40.
                         Host is up (0.014s latency).
```

Gobuster

Copyright © ForityTech

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 konfigurasi.

```
(sagiiy㉿kali)-[~/.../SecLists-master/Discovery/Web-Content/URLs]
$ gobuster dir -u 10.15.42.7 -w urls-wordpress-3.3.1.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://10.15.42.7
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 urls-wordpress-3.3.1.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s

Starting gobuster in directory enumeration mode
=====
/wp-admin/admin-post.php (Status: 200) [Size: 0]
/wp-admin/admin-footer.php (Status: 200) [Size: 2]
/readme.html (Status: 200) [Size: 7401]
/wp-admin/admin-functions.php (Status: 500) [Size: 0]
/index.php (Status: 301) [Size: 0] [→ http://10.15.42.7/]
/license.txt (Status: 200) [Size: 19915]
/wp-admin/admin-header.php (Status: 500) [Size: 0]
/wp-admin/comment.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fcomment.php&wpauth=11]
```

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.

```
.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fcredits.php&reauth=1]
/wp-admin/css/media-rtl.css (Status: 200) [Size: 26859]
/wp-admin/css/media.css (Status: 200) [Size: 26809]
/wp-admin/css/wp-admin-rtl.css (Status: 200) [Size: 490]
/wp-admin/css/wp-admin.css (Status: 200) [Size: 395]
/wp-admin/custom-background.php (Status: 500) [Size: 0]
/wp-admin/custom-header.php (Status: 500) [Size: 0]
/wp-admin/edit-form-comment.php (Status: 200) [Size: 2]
/wp-admin/edit-form-advanced.php (Status: 200) [Size: 2]
/wp-admin/css/install.css (Status: 200) [Size: 6190]
/wp-admin/edit-comments.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-
-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fedit-comments.php
&reauth=1]
/wp-admin/edit-link-form.php (Status: 200) [Size: 2]
/wp-admin/freedoms.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-logi
n.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Ffreedoms.php&reauth=1]
/wp-admin/edit-tags.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-log
in.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fedit-tags.php&reauth=
1]
/wp-admin/edit.php (Status: 302) [Size: 0] [→ http://10.15.42.7/wp-login
.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2Fedit.php&reauth=1]
/wp-admin/images/align-center.png (Status: 200) [Size: 546]
/wp-admin/images/align-left.png (Status: 200) [Size: 554]
/wp-admin/images/align-right.png (Status: 200) [Size: 509]
/wp-admin/images/align-none.png (Status: 200) [Size: 417]
/wp-admin/images/arrows.png (Status: 200) [Size: 243]
```

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.

```
└─(sagiiiy㉿kali)-[~] 68
$ nuclei -u 10.15.42.7 -o nuclei1.txt
n report for 10.15.127.69
up (0.025s latency).
n report for 10.15.127.69
up (0.025s latency).
n report for 10.15.127.249
up (0.017s latency) projectdiscovery.io
n report for 10.15.127.250
[INF] nuclei-templates are not installed, installing ...
[INF] Successfully installed nuclei-templates at /home/sagiiiy/.local/nuclei-templates (latency).
[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host lock-frontend - open (13: Permission denied) at http://lock-frontend/
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1477 (Reduced 1395 Requests) at http://lock-frontend/, ar
```

```
[missing-sri] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[report_for_10.15.127.246]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wordpress-user-enum: usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/["admin"] [latency]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 [ "["publickey","password"]"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[INF] Skipped 10.15.42.7 from target list as found unresponsive 30 times
not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
[sagiiiy@kali)-[~]
$ └─ acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), ar
at?
```

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.

```
● ● ● kessyanabrtsonianipar ~ zsh 134x24
kessyanabrtsonianipar@steph ~ % nikto -h 10.15.42.7
- Nikto v2.5.0
=====
+ Target IP:      10.15.42.7
+ Target Hostname: 10.15.42.7
+ Target Port:    80
+ Start Time:    2024-05-07 23:00:19 (GMT7)

+ Server: Apache/2.4.59 (Debian)
+ /: Retrieved x-powered-by header: PHP/8.2.18.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Link header found with value: <http://10.15.42.7/wp-json/>; rel="https://api.w.org/". See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Link
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /OORsdsKSx.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 7 item(s) reported on remote host
+ End Time:        2024-05-07 23:14:33 (GMT7) (854 seconds)
```

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.

```
sagliiy@kali: ~/wpscan
```

File Actions Edit View Help

```
| Found By: Rss Generator (Passive Detection)
| - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>
| - http://10.15.42.7/comments/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>
```

[+] WordPress theme in use: twentytwentyfour

```
| Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
| Latest Version: 1.1 (up to date)
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
| Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
| Style Name: Twenty Twenty-Four
| Style URI: https://wordpress.org/themes/twentytwentyfour/
| Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. It's a clean, modern design that's perfect for personal blogs and small websites.
| Author: the WordPress team
| Author URI: https://wordpress.org
```

```
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
```

```
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'
```

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:13 ━━━━━━ > (35 / 137) 25.5%

```
sagiiiy@kali: ~/wpscan
File Actions Edit View Help
Author URI: https://wordpress.org
Found By: Urls In Homepage (Passive Detection)
Confirmed By: Urls In 404 Page (Passive Detection)
Version: 1.1 (80% confidence)
Found By: Style (Passive Detection)
- http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'
[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:48 ━━━━━━━━ (137 / 137) 100.0%
[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: Wed May 8 04:33:34 2024
[+] Requests Done: 186
[+] Cached Requests: 7
[+] Data Sent: 44.439 KB
[+] Data Received: 21.487 MB
[+] Memory used: 279.449 MB
[+] Elapsed time: 00:01:39

(sagiiiy㉿kali)-[~/wpscan]
```

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

Blackbox Penetration Test		
Finding	Severity	Recommendation
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	Informational	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

```
Place                                     nmap -sT -p21 10.15.15.11
└─(sagiiiy㉿kali)-[~] ap scan report for 10.15.15.11
    $ ftp 10.15.42.36 21st is up (0.087s latency).
    Connected to 10.15.42.36. scan report for 10.15.15.11
    220 FTP Server                         Host is up (0.043s latency).
    Name (10.15.42.36:sagiiiy):asaggiort for 10.15.32.11
    530 This FTP server is anonymous only. latency).
    ftp: Login failed                         Nmap scan report for 10.15.40.11
    ftp> quit                                Host is up (0.024s latency).
    221 Goodbye.                            Nmap scan report for 10.15.40.11
    └─ Documents                             Host is up (0.014s latency).
```

Figure 1: Saat salah masukin name ada tulisan anonymous

```
(sagiiiy㉿kali)-[~] Setting up pkgs Nmap scan report for 10.15.75.1
$ ftp 10.15.42.36 21 Setting up gola Host is up (0.024s latency).
Connected to 10.15.42.36. Setting up gola Nmap scan report for 10.15.76.1
220 FTP Server Setting up pkgs Host is up (0.022s latency).
Name (10.15.42.36:sagiiiy): anonymous gola Nmap scan report for 10.15.77.1
331 Please specify the password. up gola Host is up (0.14s latency).
Password: Processing trig: Nmap scan report for 10.15.78.1
230 Login successful. Processing trig: Host is up (0.030s latency).
Remote system type is UNIX. Processing trig: Nmap scan report for 10.15.79.1
Using binary mode to transfer files. Host is up (0.029s latency).
ftp> ls
229 Entering Extended Passive Mode (|||65506|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May  04 15:40 backup.sql
226 Directory send OK.
ftp> █
```

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 */; 15.83.1
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */; 15.83.1
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */; 15.83.1
/*!50503 SET NAMES utf8mb4 */; 15.83.1
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */; 15.83.1
/*!40103 SET TIME_ZONE='+00:00' */; 15.83.1
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */; 15.107
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */; 15.107
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */; 15.107
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */; 15.107
-- 
-- Home             Setting up l10n Nmap scan report for 10.15.90.1
--                 Setting up golang Host is up (0.024s latency).
-- Table structure for table `users`  phys Nmap scan report for 10.15.91.1
--                 Setting up golang Host is up (0.023s latency).
--                 Setting up golang Nmap scan report for 10.15.92.1
DROP TABLE IF EXISTS `users`; 15.83.1
/*!40101 SET @saved_cs_client = @@character_set_client */; 15.93.1
/*!50503 SET character_set_client = utf8mb4 */; 15.93.1
CREATE TABLE `users` (  Processing tries Nmap scan report for 10.15.94.1
    `id` int NOT NULL,  Processing tries Host is up (0.053s latency).
    `username` varchar(255) DEFAULT NULL,  Nmap scan report for 10.15.95.1
    `password` varchar(255) DEFAULT NULL,  Host is up (0.053s latency).
    PRIMARY KEY (`id`)  | 15.95.1
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

-- 
-- Dumping data for table `users` 15.83.1
-- 
DROP TABLE IF EXISTS `users`; 15.83.1
/*!40101 SET @saved_cs_client = @@character_set_client */; 15.83.1
/*!50503 SET character_set_client = utf8mb4 */; 15.83.1
CREATE TABLE `users` (  Unpacking golang Host is up (0.051s latency).
    `id` int NOT NULL,  Selecting previous Nmap scan report for 10.15.83.1
    `username` varchar(255) DEFAULT NULL,  Host is up (0.051s latency).
    `password` varchar(255) DEFAULT NULL,  Nmap scan report for 10.15.84.1
    PRIMARY KEY (`id`)  | Selecting previous Host is up (0.045s latency).
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci; 15.83.1
/*!40101 SET character_set_client = @saved_cs_client */;

-- 
-- Selecting previous Nmap scan report for 10.15.86.1
-- Preparing to dump Host is up (0.056s latency).
-- Dumping data for table `users` 15.88.107
-- 
-- Selecting previous Host is up (0.048s latency).
-- 
-- Preparing to dump Nmap scan report for 10.15.89.1
LOCK TABLES `users` WRITE; 15.89.1
/*!40000 ALTER TABLE `users` DISABLE KEYS */; 15.89.1
INSERT INTO `users` VALUES (1,'admin','\$2y\$10\$RwYNURXBmyscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */; 15.89.1
UNLOCK TABLES; 15.89.1
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */; 15.92.1
-- 
-- Setting previous Host is up (0.053s latency).
/*!40101 SET SQL_MODE=@OLD_SQL_MODE */; 15.93.1
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */; 15.93.1
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */; 15.94.1
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */; 15.94.1
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */; 15.95.1
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */; 15.95.1
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */; 15.95.1
-- 
-- Dump completed on 2024-05-01 19:49:02

```

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

```
226 Directory send OK.      Setting up socket host is up (0.11s latency).
ftp> get backup.sql      Setting up socket Nmap scan report for 10.15.76.1
local: backup.sql remote: backup.sql host is up (0.024s latency).
229 Entering Extended Passive Mode (|||65503|) scan report for 10.15.76.1
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% [*****] 1997                                2.18 MiB/s    00:00 ETA
226 Transfer complete.      Setting up socket Host is up (0.14s latency).
1997 bytes received in 00:00 (463.00 KiB/s)  Nmap scan report for 10.15.76.1
ftp> quit                  Processing trig host is up (0.030s latency).
221 Goodbye.               Processing trig Nmap scan report for 10.15.76.1
                           Host is up (0.029s latency).

[sagiiiy㉿kali]-[~] $ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  backup.sql  nmaplog.log
```

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 mengeksplorasi 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:
[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%T=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/ ).
```

Figure 5: Penemuan 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