DEMO CORP
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: EH-001
Version 1.0
Author : Siti Nur Ellyzah

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		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
TCM Security		
Heath Adams	Lead Penetration Tester	Email: heath@tcm-sec.com

Assessment Overview

Per tanggal 5 Mei 2024 – 8 Mei 2024, CyberShield telah melakukan tes penetrasi terhadap infrastruktur Perusahaan FortifyTech. FortifyTech merupakan salah satu startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi system keamanan infrastruktur perusahaan ini.

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
Internal Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

Berdasarkan peraturan Praktikum dilarang melakukan hal-hal yang melanggar etika hacking

Client Allowances

Pengerjaan hanya bisa menggunakan jaringan ITS (dalam bentuk ***WIFI*** / ***VPN*** ITS)

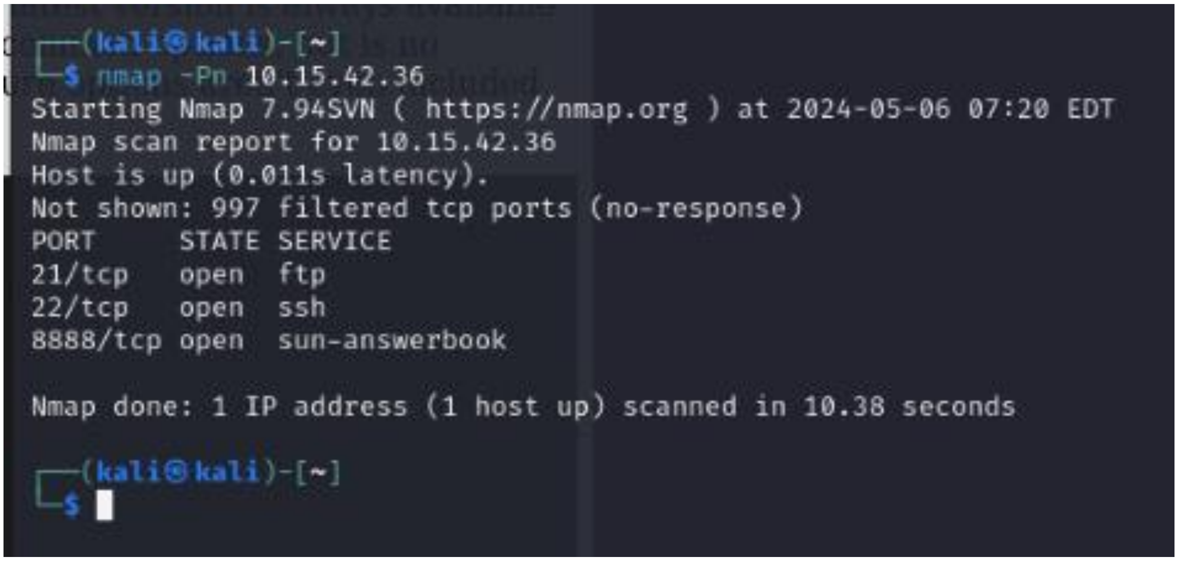
Executive Summary

CyberShield melakukan penetrasi selama kurang lebih 5 hari pengerjaan dengan beberapa hal yang sudah dilakukan dan ditemukan.

Scoping and Time Limitations

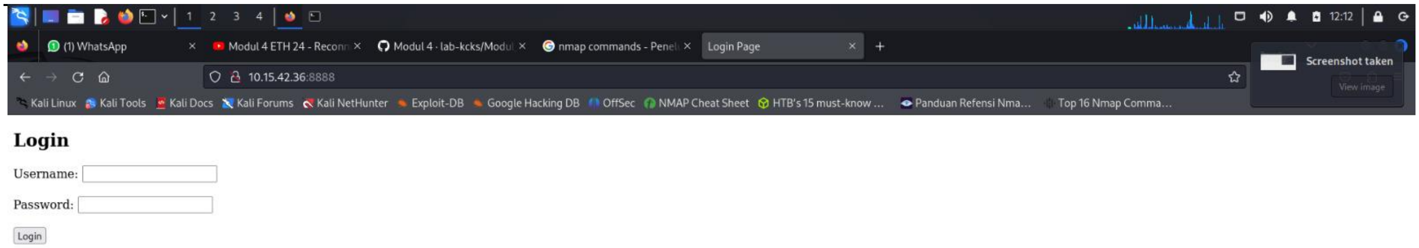
Untuk Scoping sendiri memang tidak ada ketentuan dan panduan khusus terkait apa saja yang boleh di telaah dan tidak. Serta untuk pengerjaan sendiri dilakukan selama 4 hari dengan tambahan durasi waktu 1 hari.

Testing Summary



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 07:20 EDT
Nmap scan report for 10.15.42.36
Host is up (0.011s 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: 1 IP address (1 host up) scanned in 10.38 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Pertama-tama kita lakukan scanning dengan Nmap pada scope, disini saya memilih scanning untuk scope 10.15.42.36. Dan dapat kita lihat hasil output nya pada gambar diatas. Setelahnya saya coba fokuskan pada port 8888 untuk uji coba ip address tersebut.



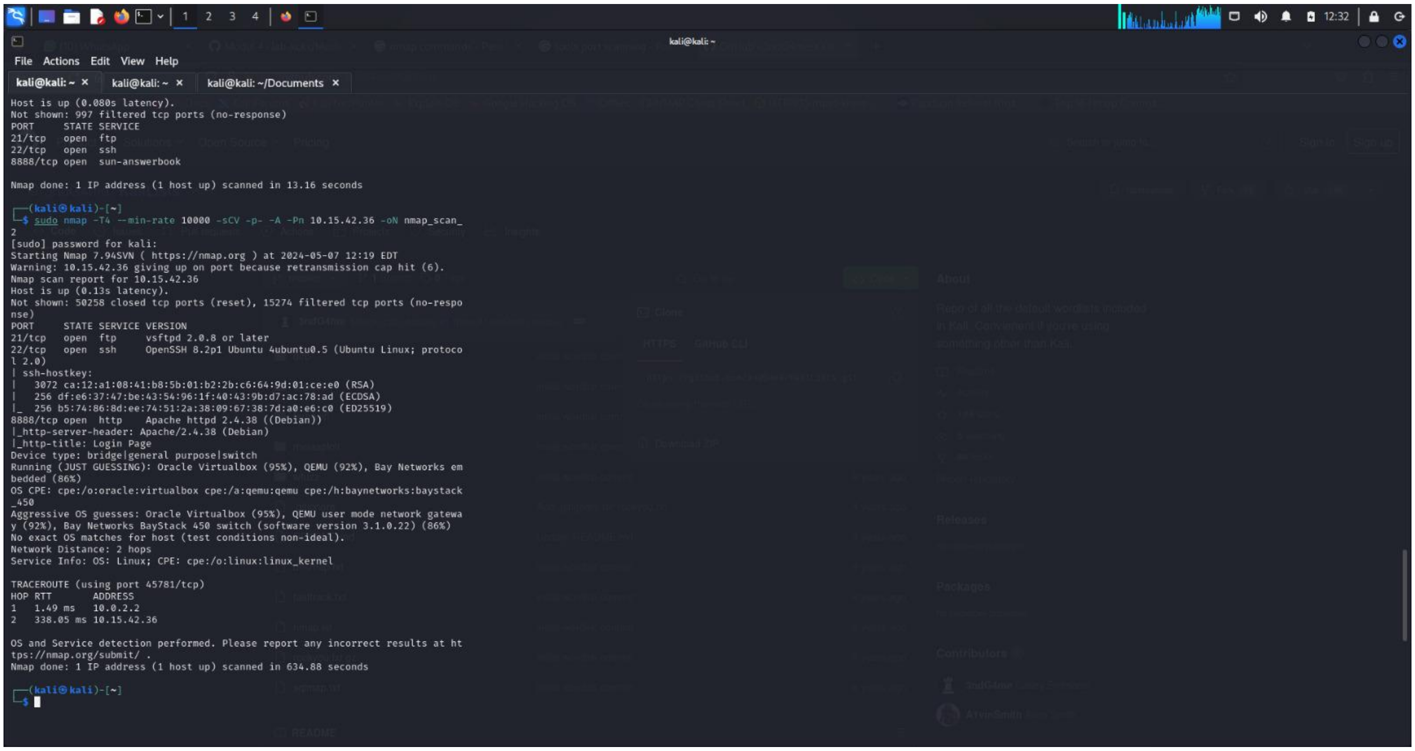
Login

Username:

Password:

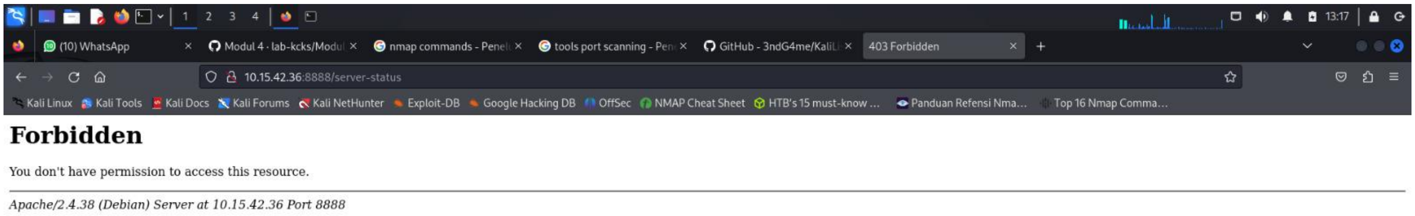
Login

Dan setelahnya saya temukan laman login seperti ini yang setelah saya cek di Network memang zonk (alias tidak ditemukan sesuatu hal yang dirasa vulnerable).



```
Host is up (0.080s 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: 1 IP address (1 host up) scanned in 13.16 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -T4 --min-rate 10000 -sCV -p- -A -Pn 10.15.42.36 -oN nmap_scan_
2
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 12:19 EDT
Warning: 10.15.42.36 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.36
Host is up (0.13s latency).
Not shown: 50258 closed tcp ports (reset), 15274 filtered tcp ports (no-respo
nse)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login Page
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (92%), Bay Networks em
bedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack
_450
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gatewa
y (92%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 45781/tcp)
HOP RTT       ADDRESS
1   1.49 ms   10.0.2.2
2   338.05 ms 10.15.42.36

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 634.88 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Dan ini dengan menggunakan command yang lebih mendetail, hasil output seperti yang tertera diatas.



Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 10.15.42.36 Port 8888

Ketika dilakukan pengecekan server-status, 10.15.42.36:8888 hasilnya adalah dilarang yang berarti akses terlarang untuk resource alamat ini.

Tester Notes and Recommendations

Kesimpulan yang bisa diambil ialah dirasa bahwa vulnerabel yang ditemukan tidak termasuk dalam tingkat yang berbahaya.

Dirasa ada beberapa tahapan atau steps yang membutuhkan waktu yang sangat lama jadi bisa dilakukan beberapa tahap dalam satu waktu yang bersamaan agar tidak saling menunggu.

Key Strengths and Weaknesses

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		

Technical Findings

Internal Penetration Test Findings

Last Page