FortifyTech
Security Assessment
Findings Report

Asadel Naufaleo (5027221009)

Date:
May
8th,
2024

Pernyataan Kerahasiaan

Dokumen ini dibuat oleh Asadel Naufaleo sebagai penguji *pentest* dari Mahasiswa Teknologi Informasi ITS sebagai bagian dari asesmen *Ethical Hacking*. Dokumen ini berisi laporan kerentanan serta celah keamanan dari system *FortifyTech* dengan izin dan sepengetahuan dari pihak yang terlibat serta mengandung informasi-informasi tertutup dari pihak yang bersedia untuk dijalankan tes ini.

Disclaimer

Penetration Test ini dilakukan dengan *consent* penuh dari pihak yang bersangkutan yaitu *FortifyTech*. Segala penemuan yang ditemukan oleh penguji telah dimuat dalam dokumen ini sebagai perjanian awal mengenai kerahasiaan dan sebagai tanda kepatuhan terhadap *MOU* antara kedua pihak.

Contact Information

Nama: Asadel Naufaleo
No.Telp: 5027221009
Email: a.naufaleo@gmail.com
Status: Mahasiswa Teknologi Informasi ITS

Assesment Overview

Tujuan utama dari praktikum ini adalah untuk mengidentifikasi kerentanan dalam infrastruktur FortifyTech dengan menggunakan prinsip-prinsip Ethical Hacking. Dengan mensimulasikan serangan dunia nyata, penilaian bertujuan untuk mengungkap kelemahan yang dapat dimanfaatkan oleh pihak jahat untuk mengkompromi keamanan dan integritas sistem FortifyTech.

Fase aktivitas *Penetration Testing* termasuk sebagai berikut:

- Planning – Merencanakan dan mengumpulkan informasi mengenai target.
- Discovery – Melakukan *scanning* dan *enumeration* untuk mendeteksi kemungkinan kerentanan serta celah keamanan pada *website*.
- Attack – Melakukan eksploitasi pada sisi lemah dan celah keamanan yang ada.
- Reporting – Mendokumentasikan semua penemuan kerentanan, hasil eksploitasi, serta semua yang berkaitan dengan informasi *penetration test* yang dilakukan.

Assesment Components

Blackbox Penetration Test

Blackbox Penetration Test adalah tipe *pentest* dimana penguji hanya diberikan informasi yang minim mengenai target atau website yang akan diuji. Pada kasus ini, penguji hanya mendapatkan informasi awal berupa link dari website tersebut. Penguji tidak diberikan info lain selain dari informasi tersebut, sehingga pengujian ini lebih mensimulasikan kondisi yang realistis dimana penyerang dari luar tidak memiliki informasi apapun.

Severity Rating

Severity	CVSS V3 Score Range	Defini tion
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.

Scope

Assessment	Details
Blackbox Penetration Test	• 10.15.42.36 • 10.15.42.7

Client Allowances

Pihak yang diuji (*FortifyTech)* tidak memberikan Batasan mengenai pengujian yang dilakukan, sehingga penguji dapat melakukan metode-metode apapun.

Executive Summary

Penguji telah mengevaluasi kemanan system *website FortifyTech* melalui *Penetration Testing* efektif dari tanggal 5 May 2024 sampai 8 May 2024. Pada bagian-bagian berikut telah disajikan berbagai ringkasan mengenai penemuan kerentanan, keberhasilan dan kegagalan eksploitasi, juga kelebihan dan kekurangan dari system.

Scoping and Time Limitations

Scoping selama pengujian adalah tidak adanya Batasan oleh *client* mengenai pengujian pada seluruh komponen pengujian.

Batas waktu telah ditentukan untuk pengujian. *Blackbox Penetration Testing* telah diizinkan untuk dilakukan selama 3 hari.

Testing Summary

Pengujian dilakukan dengan informasi awal yang diberikan adalah 2 IP Address untuk diakses yaitu 10.15.42.36 dan 10.15.42.7. Pada link pertama yaitu 10.15.42.36 jika dibuka pada browser, link tersebut tidak menunjukkan apapun. Oleh karena itu, penguji mencoba menggunakan nmap pada link tersebut.

Hasil scanning dari nmap memberikan informasi yang cukup penting, dimana diketahui bahwa terdapat 3 open port dengan berbagai tipe. Penguji berhasil mengakses port 8888 pada browser dan ditemukan suatu laman login. Hasil dari tersebut tidak menemukan hal yang cukup penting sejauh ini. Penguji juga mencoba salah satu port lain yang terbuka yaitu port 21 dengan tipe ftp. Pada port tersebut, penguji juga berhasil login pada ftp setelah beberapa percobaan, dan diketahui bahwa *username* yang digunakan cukup awam dan terdapat kerentanan pada *password* dimana orang yang mengakses akun tersebut tanpa menginputkan apapun pada kolom *password* maupun mengisinya dengan kata *random,* sistem akan tetap menganggap percobaan login tersebut s*uccessful*.

Pada port tersebut, penguji dapat mengakses file yang ada di dalamnya. Penguji juga menemukan sebuah file Bernama "*backup.sql".* File tersebut merupakan hasil dari server sql. Jika dibaca dari *conversation* pada sistem, terdapat percobaan login yang berhasil. Dan jika kita buka file tersebut terdapat percobaan login yang dengan *username* "admin" dengan *password* yang telah di-hash. Penguji telah mencoba menggunakan john the ripper untuk memecahkan hash dari password tersebut namun tidak berhasil. Namun, celah keamanan tersebut sangatlah rentan untuk sistem, dan jika diberi waktu yang lebih Panjang, penyerang dapat melakukan eksploitasi yang lebih *critical*.

Pada link kedua, yaitu 10.15.42.7, dapat diakses langsung melalui browser. Link tersebut mengarahkan ke suatu *homepage* laman *Wordpress.* Mengetahui website tersebut menggunakan wordpress, penguji menggunakan WPScan untuk mendapatkan informasi lebih dalam mengenai sistem dan kerentanan yang ada pada laman tersebut. Hasil dari WPScan menemukan adanya readme.html yang dapat diakses langsung dari link. Diketahui juga website tersebut menyalakan XML_RPC, WP-Cron. Juga ditemukan adanya robots.txt. Pada website tersebut juga dapat melakukan comment maupun post, dan untuk traffic dapat di intercept menggunakan burpsuite sehingga dapat melakukan manipulasi request kepada sistem, dimana bisa menjadi celah keamanan.

Karena keterbatasan waktu, penguji tidak dapat melakukan diagnosa lebih dalam pada kedua website. Namun sejauh ini, kerentanan yang ditemukan dapat dikatakan cukup penting dan perlu diinformasikan pada pihak yang diuji untuk dilakukan evaluasi terhadap celah-celah keamanan tersebut.

Key Strengths and Weaknesses

Berikut adalah kunci kelebihan pada *assessment* yang dilakukan:

1. Menyalakan fitur XML-RPC
2. Menggunakan WP-Cron
3. Menggunakan hashing pada penggunaan *password user*-nya

Berikut adalah kunci kelemahan pada *assessment* yang dilakukan:

1. Penggunaan *username* yang umum sehingga mudah ditebak
2. Kelemahan password pada port 21 ftp dimana dapat diakses dengan input apapun
3. Terbukanya file penting pada *surface level*, yaitu backup.sql
4. Terbukanya isi backup.sql yang berisi *username* serta *password*
5. Adanya celah melalui robots.txt

Vulnerability Summary & Report Card

Berikut merupakan tabel yang mengilustrasikan kerentanan yang ditemukan berdasarkan dampak dan rekomendsinya.

Blackbox Penetration Test Findings

0	3	0	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Blackbox Penetration Test		
BPT-001: Port 21 ftp yang terbuka dengan akses yang mudah	High	Menggunakan *username* dan *password* yang unik dan tidak awam
BPT-002: File sql yang terekspos pada *surface level security*	High	Menyimpan file-file yang berkaitan dengan data pada folder yang lebih aman dan membutuhkan akses tinggi
BPT-003: File sql yang berisi *username* dan *password* dari admin	High	Mengevaluasi file yang dapat diakses oleh role tertentu
BPT-004: Penemuan port yang terbuka	Informational	Mereview aksi dan tahap remediasi

Technical Findings

Blackbox Penetration Test Findings

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

Description:	Pada link pertama 10.15.42.36, setelah penguji menemukan port yang terbuka, penguji dapat dengan mudah mengakses port-port tersebut, dan salah satunya adalah port 21 ftp. Pada port tersebut diperlukan login dan penguji berhasil login dengan menebak *username* dengan kata yang cukup awam. Kerentantan lainnya juga adalah tidak adanya pengecekan pada input password sehingga jika kolom tersebut kosong ataupun diisi dengan kata apapun, maka sistem akan tetap "Login Successful"
Risk:	Mudahnya akses oleh penyerang dengan intensi jahat untuk mendapatkan akses pada *role* yang lebih tinggi
System:	All
Tools Used:	Nmap, John the ripper

Evidence:

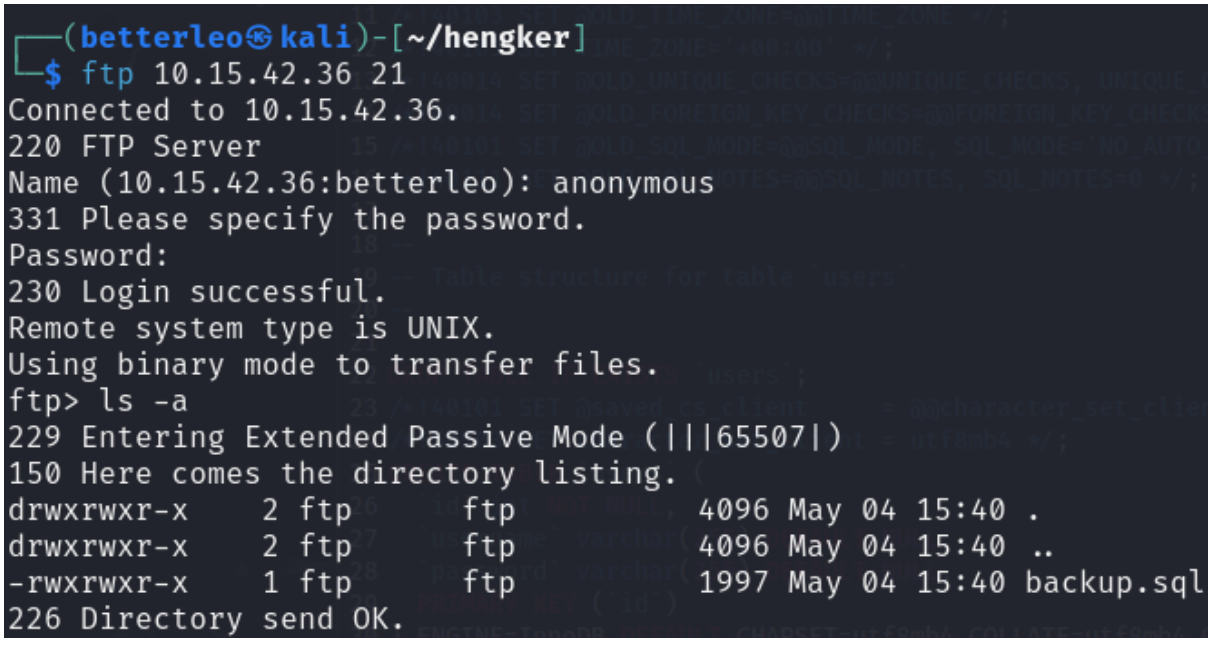
```
┌──(betterleo㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 14:09 WIB
Nmap scan report for 10.15.42.36
Host is up (0.0083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Network
s BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 19.48 seconds
```

Remediation:
Menggunakan username dan password yang unik dan tidak awam agar tidak mudah ditebak oleh penyerang dari luar.

Finding BPT-002: File sql yang terekspos pada surface level security

Description:	Pada link pertama 10.15.42.36 yang sama, pada port 21 yang telah berhasil login terdapat 1 file yang terlihat pada *surface level* yaitu file Bernama backup.sql. File tersebut dapat dilihat dengan command “ls -a” tepat setelah berhasil login.
Risk:	Penyerang dapat dengan mudah mengakses file-file lainnya dan membaca file yang terekspos. File tersebut juga dapat didownload oleh penyerang sehingga dapat diproses lagi data-datanya sebagai pengumpulan informasi, terlebih lagi apabila informasi yang dikandung merupakan informasi sensitive.
System:	All
Tools Used:	Nmap

Evidence:



Remediation:

Menyimpan file-file yang berkaitan dengan data pada folder yang lebih aman dan membutuhkan akses tinggi

Finding BPT-003: File sql yang berisi *username* dan *password* dari admin

Description:	Melanjutkan step sebelumnya, file yang dapat diakses dan didownload tadi yaitu “backup.sql” diproses dan dianalisa isinya. Pada file tersebut diketahui terdapat percobaan login yang berhasil dengan username “admin” dengan password yang telah di-hash.
Risk:	Jika penyerang memiliki banyak waktu, password yang telah di-hash dapat diretas dan diketahui bentuk aslinya dengan menggunakan wordlist yang telah disiapkan.
System:	All
Tools Used:	Nmap, John The Ripper, Hashmap

Evidence:

```
-- 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`
--

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 */;
```

Remediation:

Mengevaluasi file yang dapat diakses oleh role tertentu

Finding BPT-004: Penemuan port yang terbuka

Description:	Melanjutkan step sebelumnya, file yang dapat diakses dan didownload tadi yaitu “backup.sql” diproses dan dianalisa isinya. Pada file tersebut diketahui terdapat percobaan login yang berhasil dengan username “admin” dengan password yang telah di-hash.
Risk:	Jika penyerang memiliki banyak waktu, password yang telah di-hash dapat diretas dan diketahui bentuk aslinya dengan menggunakan wordlist yang telah disiapkan.
System:	All
Tools Used:	Nmap, John The Ripper, Hashmap

Evidence:

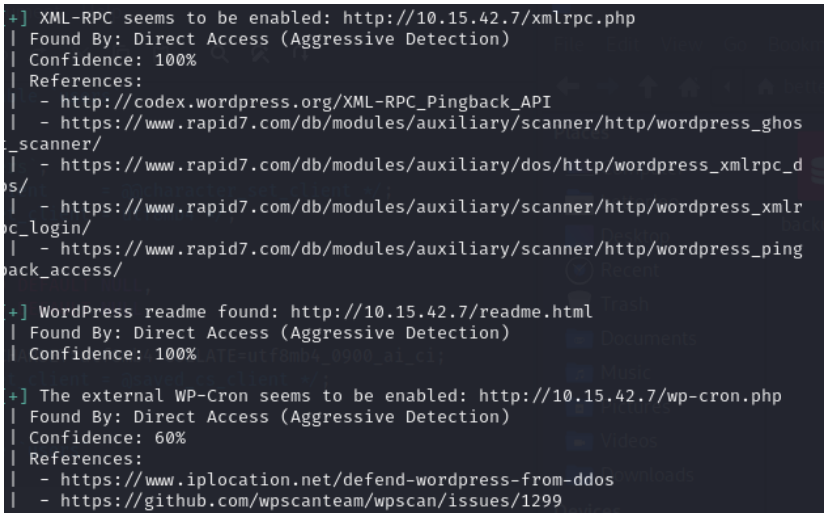
```
┌──(betterleo㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 14:09 WIB
Nmap scan report for 10.15.42.36
Host is up (0.0083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Network
s BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 19.48 seconds
```

Remediation:

Mereview aksi dan tahap remediasi

Dokumentasi lain mengenai informasi

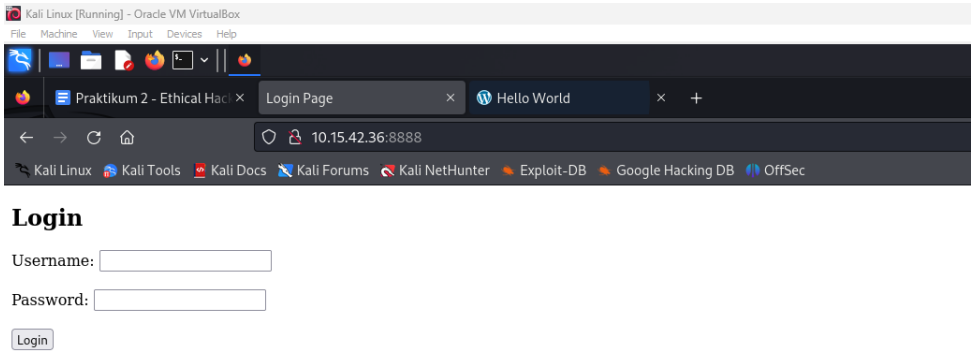
Hasil scan WPScan

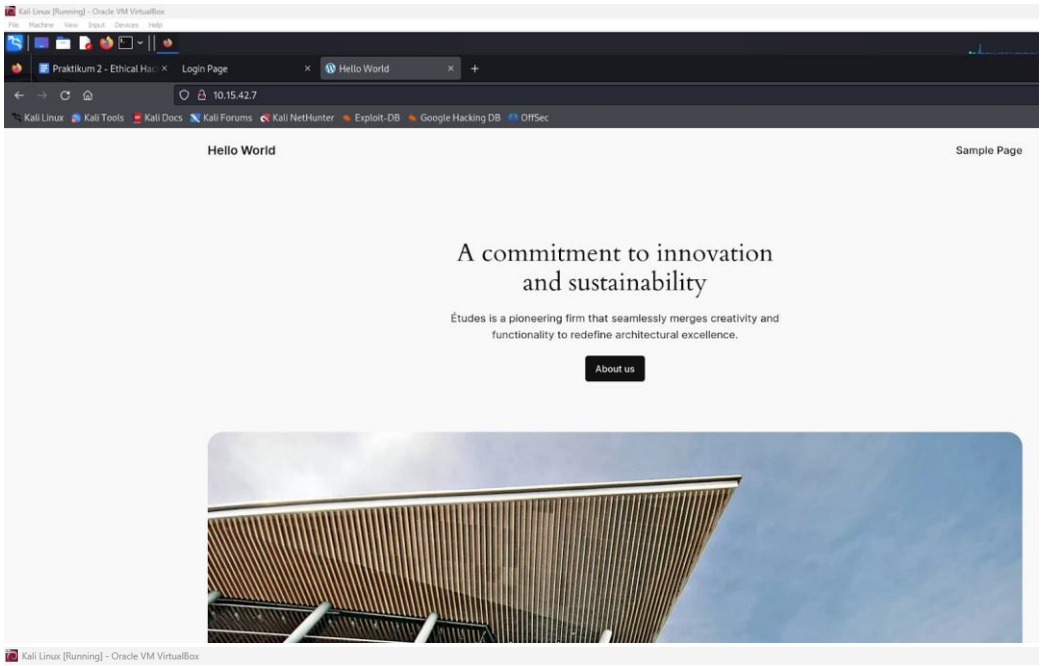


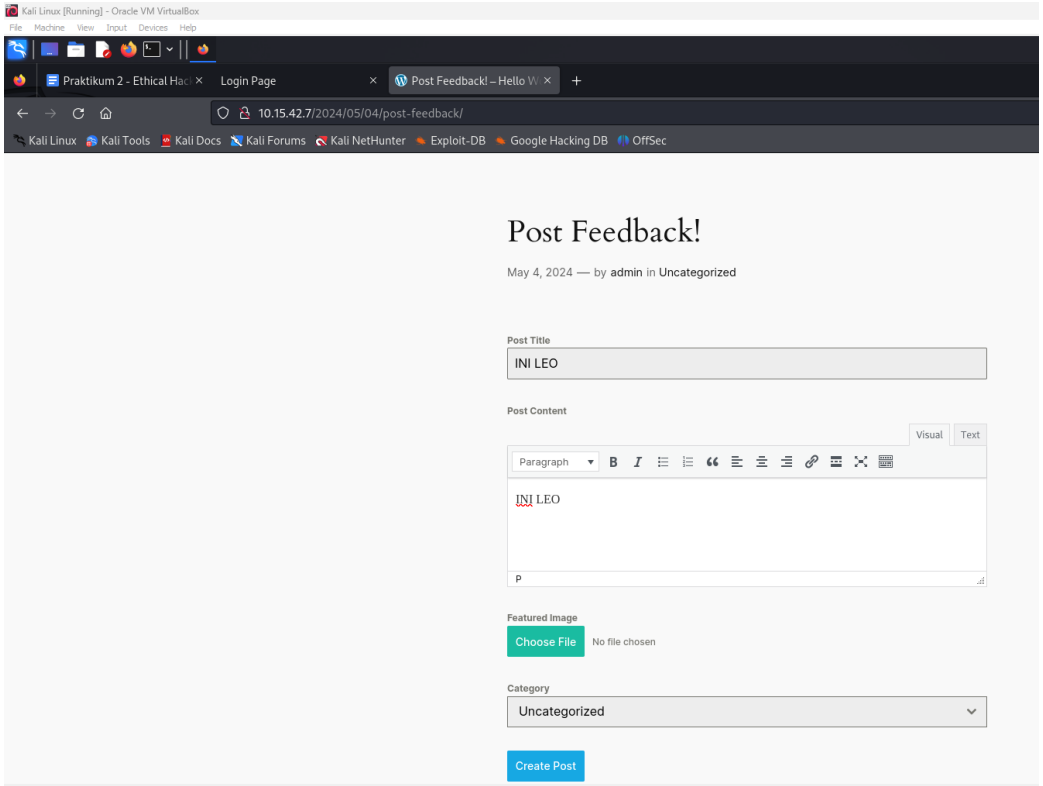
Hasil Nmap link 10.15.42.7

```
┌──(betterleo㉿kali)-[~]
└─$ sudo nmap -sV -O 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 15:10 WIB
Nmap scan report for 10.15.42.7
Host is up (0.0046s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (91%), 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 (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 17.18 seconds
```

Tampilan kedua website




Kali Linux [Running] - Oracle VM VirtualBox
Praktikum 2 - Ethical Hac
Login Page
Hello World
10.15.42.7
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hello World
Sample Page
A commitment to innovation and sustainability
Études is a pioneering firm that seamlessly merges creativity and functionality to redefine architectural excellence.
About us


Kali Linux [Running] - Oracle VM VirtualBox
Praktikum 2 - Ethical Hac
Login Page
Post Feedback! – Hello W
10.15.42.7/2024/05/04/post-feedback/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Post Feedback!
May 4, 2024 — by admin in Uncategorized
Post Title
INI LEO
Post Content
Visual
Text
Paragraph
INI LEO
P
Featured Image
Choose File
No file chosen
Category
Uncategorized
Create Post

Last Page