LAPORAN PRAKTIKUM I
KEAMANAN INFORMASI

Disusun Oleh :

Nama : Taufan Ali

NIM : 2215016135

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI TERAPAN

UNIVERSITAS AHMAD DAHLAN

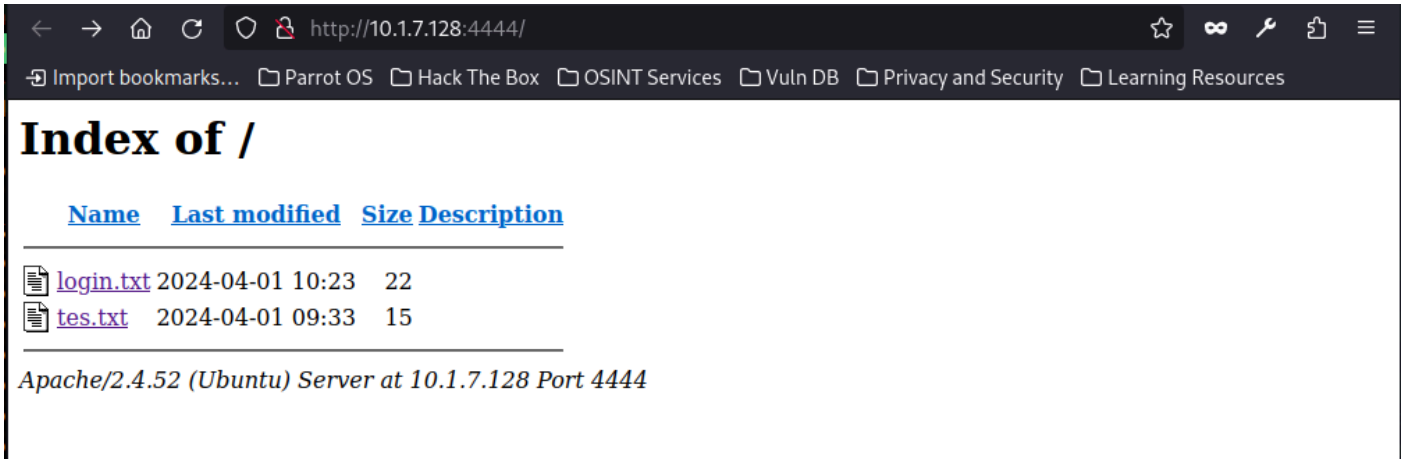
2024

Pertama lakukan scanning pada ip target(10.1.7.128) menggunakan tools nmap untuk melihat port mana saja yang terbuka.

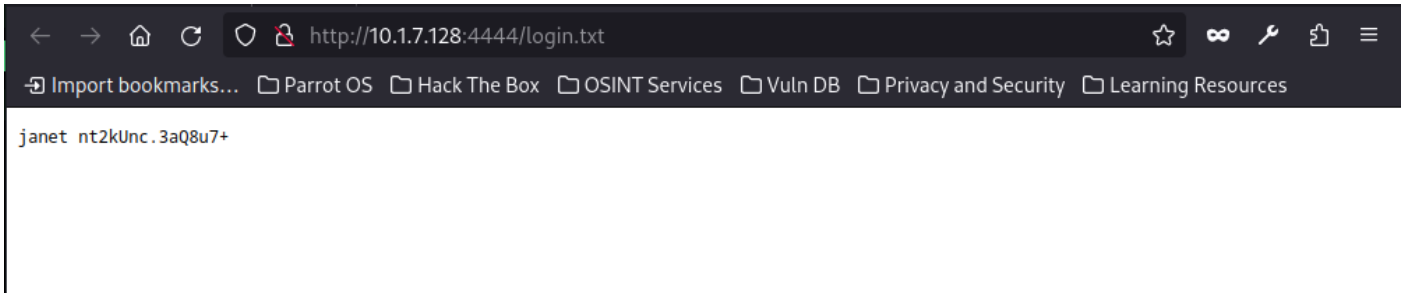
```
alienz65@parrot ~ sudo nmap -P 10.1.7.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 13:00 WIB
Nmap scan report for 10.1.7.128
Host is up (0.0037s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
1234/tcp open  hotline
4444/tcp open  krb524
8888/tcp open  sun-answerbook
9090/tcp open  zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
alienz65@parrot ~
```

Kita coba tes port mana saja yang dapat diakses dari browser dengan mengetikkan ip_target:port_yang_dicek. Setelah melakukan pengecekan semua port, ditemukan 1 port yang berisikan 2 file dan dapat diakses yaitu port 4444



Dalam port 444 terdapat file login.txt yang saya curigai merupakan username dan juga password untuk masuk kedalam sesuatu, sayangnya saya tidak tahu username dan password tersebut dapat digunakan untuk masuk kemana. Saya telah mencoba untuk melakukan login kedalam ssh dan ftp menggunakan username dan password namun tidak juga berhasil.



Kesimpulannya, menyimpan file pada sebuah port yang terbuka dapat menyebabkan terjadinya kerentanan jika disalahgunakan