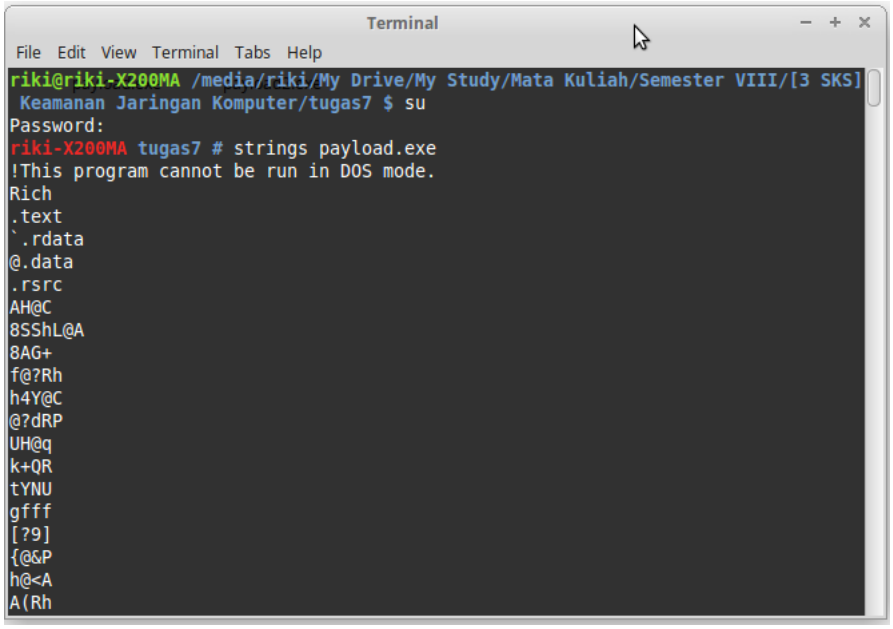
Nama : Riki Andika
NIM : 09011181320015

Hang on Training, Kamis 30 Maret 2017

Analisis File Payload

a. File Payload 1

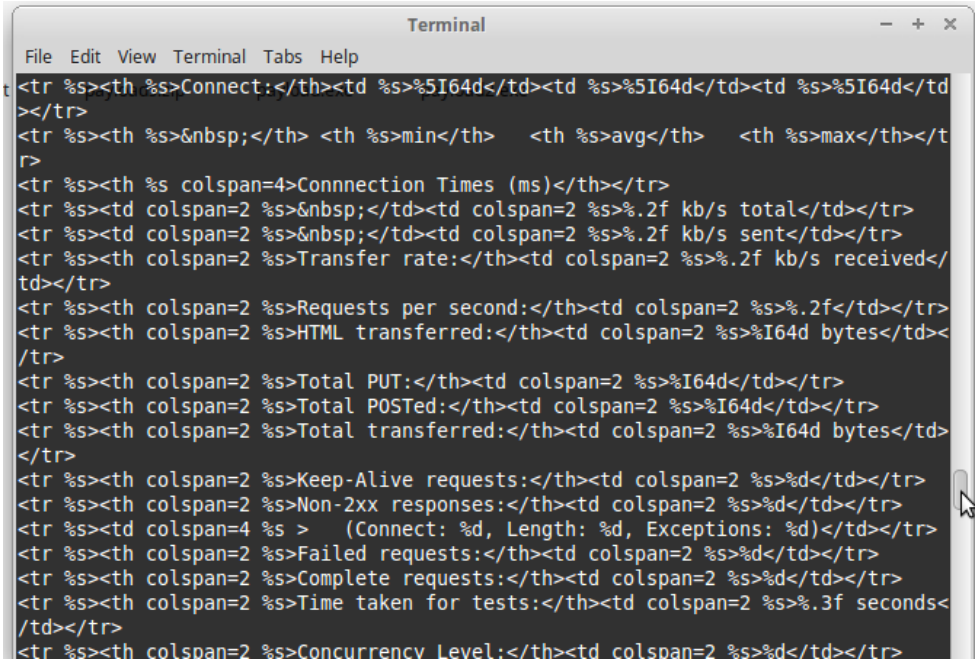
Payload ini merupakan aplikasi apachebench yang ada didalam aplikasi dengan format exe, hal ini terlihat ketika aplikasi payload.exe dijalankan dengan menggunakan tools ghex dan strings, yang berisi informasi-informasi mengenai aplikasi apachebanch, seperti yang terlihat pada gambar 1, dengan informasi yang didapat sebagai berikut;



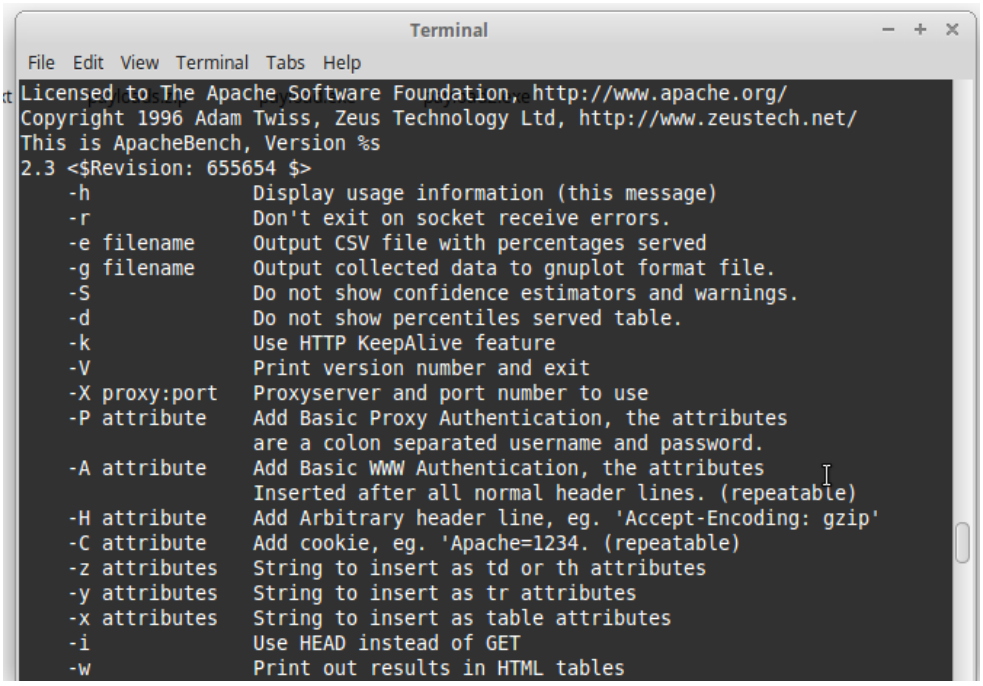
Gambar 1. Menjalankan payload 1 dengan string

Apachebanch merupakan tool untuk mengukur performance apache, dengan apachebanch dapat melihat kapabilitas apache untuk melayani request dari client. Apachebanch ini telah terinstall secara otomatis ketika menginstall Apache HTTP Server, jika apache sudah terinstall maka tool benchmarking ini juga sudah otomatis ada. Lokasi tool ab ini biasanya berada didalam direktori, tool apachebench ini bisa digunakan tidak hanya untuk Apache, tapi untuk web server lain juga seperti Lighthttpd,

Nginx atau Miscrosoft II. Berukut informasi dari file payload.exe yang menunnjukkan bahawa file payload.exe adalah apachebanch, pada gambar 2 dan 3 berikut;



Gambar 2. Code html dari apachebanch

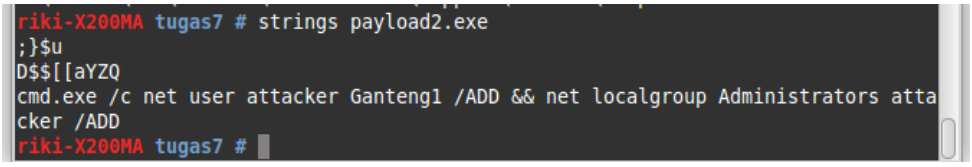


Gambar 3. Informasi dari payload 1 (Apachebanch)

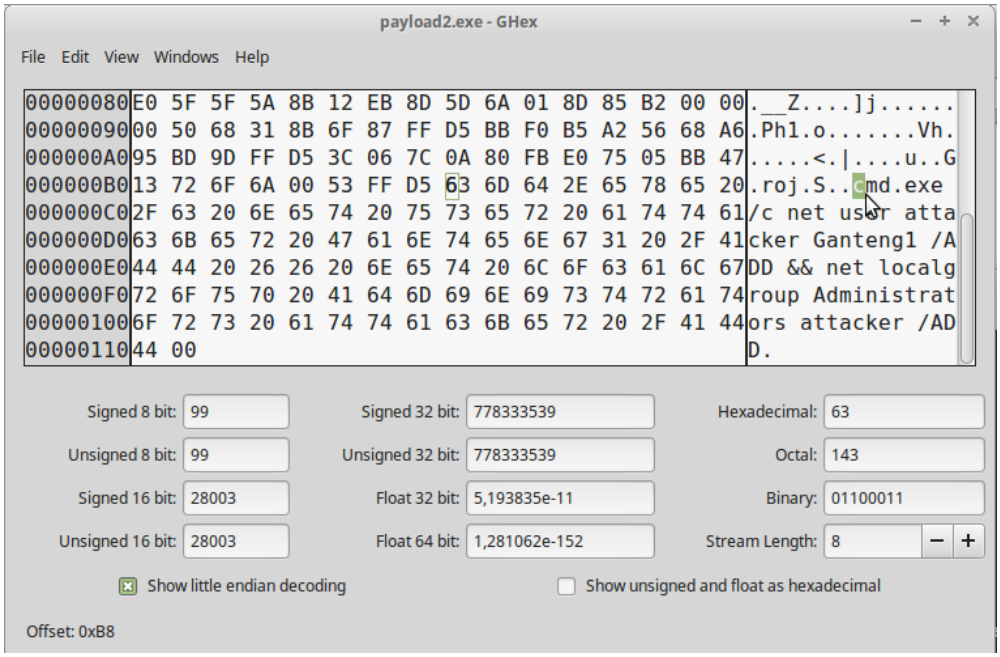
b. File Payload 2

File payload dua ini merupakan exploid yang dibuat dengan extention exe, dimana didalam file payload2.exe ini berisi program dengan informasi-informasi yang mendekati dari serangan exploit. Exploit adalah sejenis software atau aplikasi yang dibuat untuk menyerang kelemahan dalam sebuah sistem secara spesifik untuk mendapatkan akses dari user admin dan menginfeksi target yang deserang. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Biasanya exploit mencari kelemahan dari variabel null ataupun variabel yang tidak terdefinisi untuk dimasukkan nilai lain sehingga terjadi error dan tidak membaca prosedur program seperti seharusnya, sehingga shellcode dapat dimasukkan untuk melaksanakan perintah atau command lainnya.

Pada local exploit, sejak awal attacker sudah memiliki shell access baik melalui ssh, telnet atau remote desktop connection, namun dengan hak akses terbatas (sebagai normal user). Sedangkan pada remote exploit, kondisi awal attacker adalah tidak memiliki akses shell. Akses shell yang saya maksud adalah kemampun untuk execute suatu file executable. Local Exploit merupakan program atau eksploit yang jika dijalankan pada mesin atau target yang telah hack sebelumnya dengan sasaran server itu sendiri yang akan mengakibatkan hacker untuk mendapatkan root shell di mesin/server sasaran yang berarti mempunyai akses root dimesin (hak akses yang terbatas lalu menjadi tidak terbatas).



Gambar 4. Payload 2



Gambar 5. Menjalankan file payload2.exe dengan tool ghex