*Heartbleed bug* pertama kali ditemukan oleh peneliti dari *Codenomicon* dan*Google*, Neel Mehta, pada Jumat 11 April kemarin. *Bug* sendiri “diciptakan” oleh Robin Seggelmann yang dulunya juga bekerja dalam proyek OpenSSL pada 2008 hingga 2012 lalu.

Heartbleed adalah celah keamanan di salah satu ekstensi OpenSSL yang disebut Heartbeat. Celah keamanan ini memungkinkan attacker untuk membaca memory dari server yang diproteksi oleh OpenSSL. Sehingga membuat hacker bisa mendapatkan seluruh isi dari memory (RAM) pada server yang besarnya sampai 64KB. Heartbleed berasal dari implementasi protokol heartbeat (RFC6520) TLS/DTLS (Transport Layer Security Protocols).

KESIMPULAN : ***“Bug* ini menyerang standar enkripsi OpenSSL yang umumnya digunakan untuk menyimpan data dan informasi sensitif, seperti password, username, dan informasi kartu kredit pengguna dengan jangkauan yang luas.”**

Dampak dari [bug Heartbleed](http://www.gantengers.web.id/2014/12/temuan-bug-vulnerability-heartbeat-pada-openssl.html) ini adalah adanya over run pada extinsion heartbeat karena tidak dilakukannya bound cheking. over run ini juga bisa dimanfaatkan unuk mengintip isi memori hingga 64.000 untuk user atau client server yang mengkoneksikan nya ke server website yang vuln terhadap heartbeat. Dan berikut ini penampakan dari isi memori tersebut.

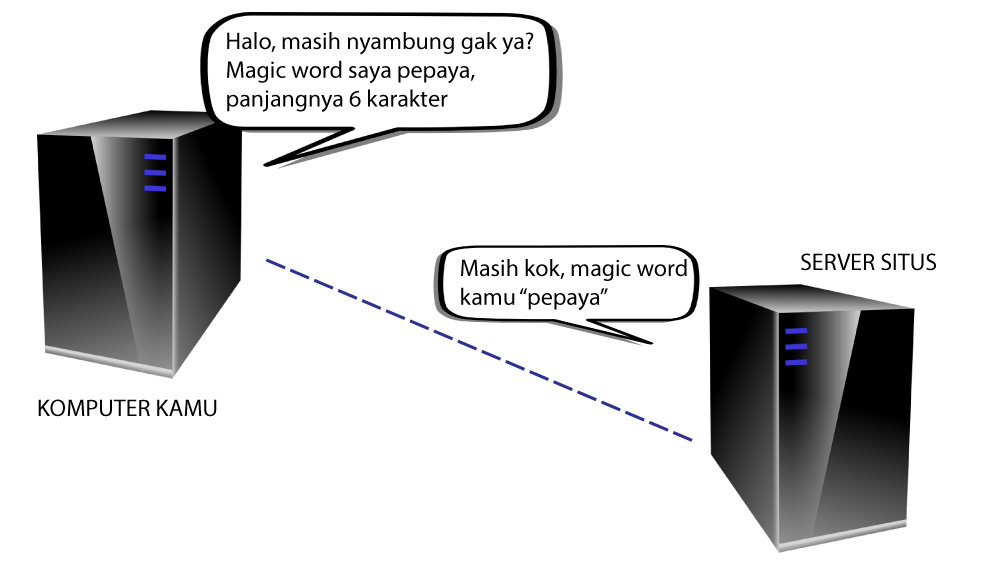
1. Cookie Website
2. Source Code Script
3. Kombinasi Username Dan Password
4. Kunci Pribadi OpenSSL

**Beberapa pengertian yang salah Seputar *Heartbleed*:**

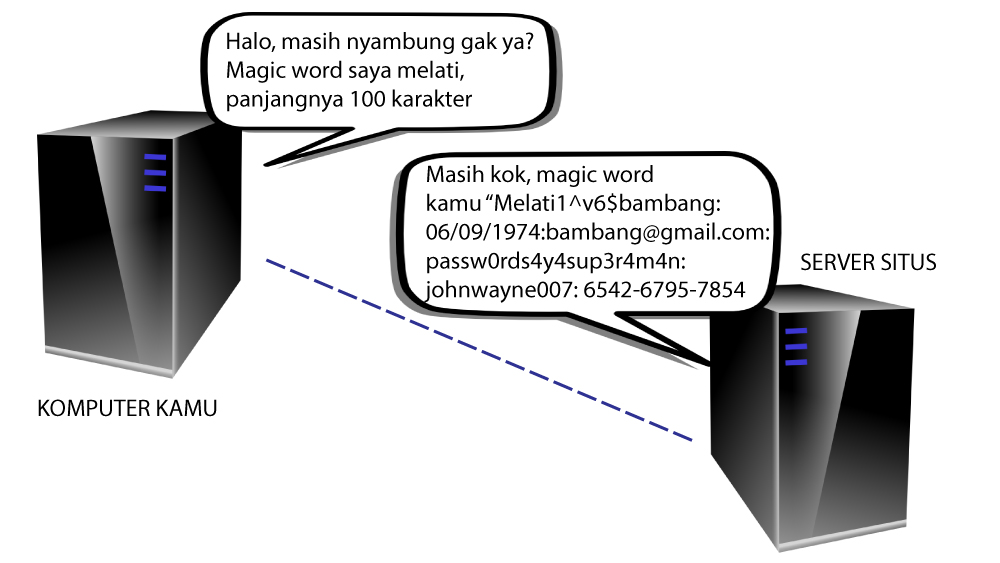
1. **Heartbleed bukanlah virus**. Heartbleed adalah bug di ekstensi Heartbeat OpenSSL versi 1.0.1 sampai 1.0.1f
2. **Update antivirus tidak akan berpengaruh** terhadap kebal atau tidaknya perangkat gadget terhadap Heartbleed karena Heartbleed bukanlah virus dan dia tidak menyebar atau menginfeksi perangkat atau PC kita.
3. **Mengganti password tetap tak menjamin dan salah, jika situs yang Anda gunakan itu belum kebal terhadap Heartbleed.** Ganti password Anda setelah situs tersebut di patch dan kebal terhadap Heartbleed. Mengganti password sebelum situs tersebut kebal terhadap Heartbleed sama artinya dengan memberikan kesempatan kepada sang attacker untuk mencuri detail password baru Anda.

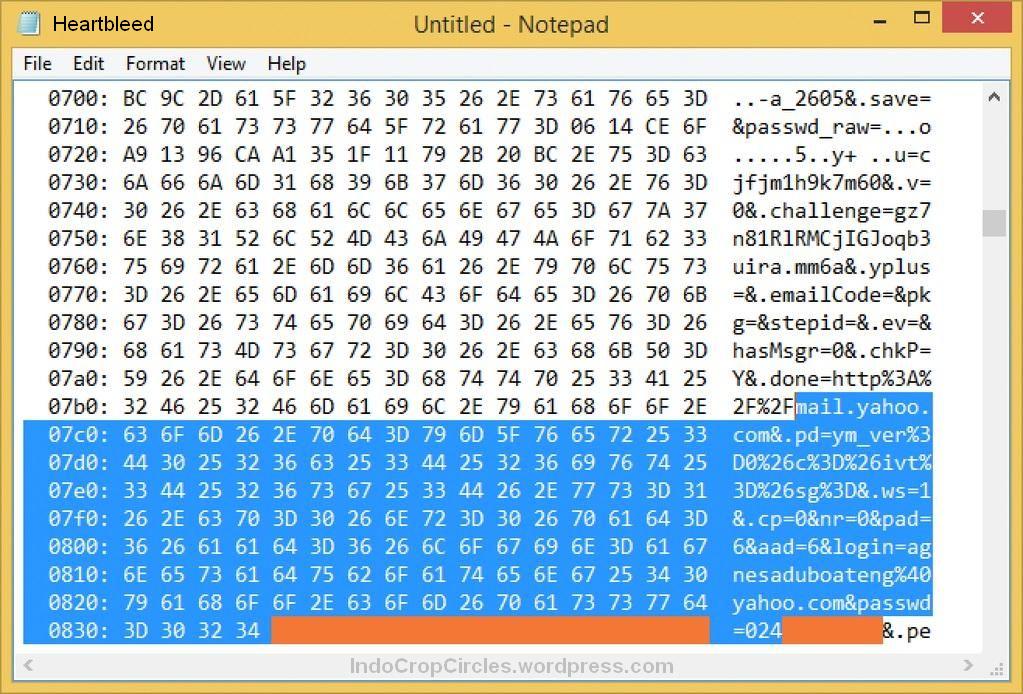
**Cara Kerja dari Heartbleed**

1. Komputer Hacker (Kamu) akan mengirimkan pesan berisi sebuah “KATA” dan “JUMLAH KARATER KATA” , kemudian server akan membalas pesan tersebut dengan balasan “KATA” yang diminta dari komputer kamu.



1. Kemudian dari pada itu Komputer Hacker (Kamu) hanya mengirimkan sebuah kata yang pendek seperti “melati” tetapi Hacker meminta respon kepada server sebanyak 100 karakter. Server tidak mengecek jika kata “melati” hanya memiliki 6 karakter maka server langsung “memuntahkan” semua karakter yang tersimpan di memori RAM-nya untuk memenuhi permintaan 100 karakter. (Hacker bukan hanya meminta 100 karakter tetapi bisa sampai 64.000 karakter). Dari situlah hacker mendapat username dan password si pemilik.





Inilah tampilan “Heartbleed bug” yang sedang digunakan cracker saat meretas. Sudah lebih dari dua tahun yang lalu, Heartbleed bisa memberikan celah bagi siapa saja untuk mengeksploitasi sebuah situs dengan protokol OpenSSL.

Celah ini memberi kesempatan bagi penjahat *cyber* untuk mengintai pengguna komputer yang mengakses situs terinfeksi Heartbleed, selama ia masih terkoneksi ke internet. Ini dikenal dengan ekstensi Heartbeat. Tapi sinyal berbahaya dari Heartbeat bisa memaksa pembocoran data untuk mengungkap informasi rahasia yang tersimpan di memori.

Dan kemungkinan kejahatan yang bisa dilakukan adalah pencurian *username* dan *password*. Penjahat *cyber* bisa menggunakan *username* dan *password* tersebut untuk menyalahgunakan sebuah akun layanan tertentu.

Referensi:

* <https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fwinpoin.com%2Fapa-itu-heartbleed-bagaimana-cara-mengatasinya-dan-kabar-sesat-mengenainya%2F&ei=zAtwVcuVJsytuQSeqoCIDA&usg=AFQjCNEtOjSZIa2xULkm65AiA_4wxWxkpg&sig2=VAHM8IocmXLzkthnK1ORbw>
* <http://utekno.com/apakah-itu-heartbleed-5832>
* <http://internetivis.blogspot.com/2014/04/pengertian-heartbleed.html>
* <http://www.gantengers.web.id/2014/12/temuan-bug-vulnerability-heartbeat-pada-openssl.html>
* <http://okepram.blogspot.com/2014/04/heartbleed-buat-internet-loyo-bahayakan.html>