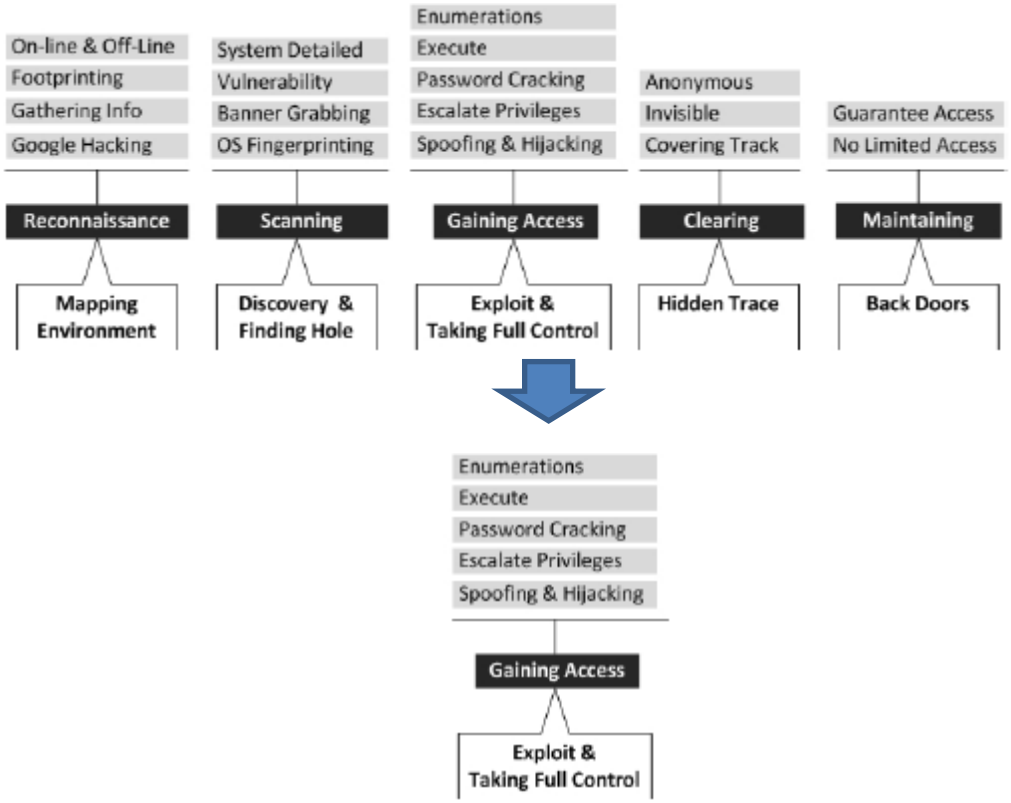
TUGAS KEAMANAN JARINGAN KOMPUTER
EXPLOIT

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
2017

Exploit

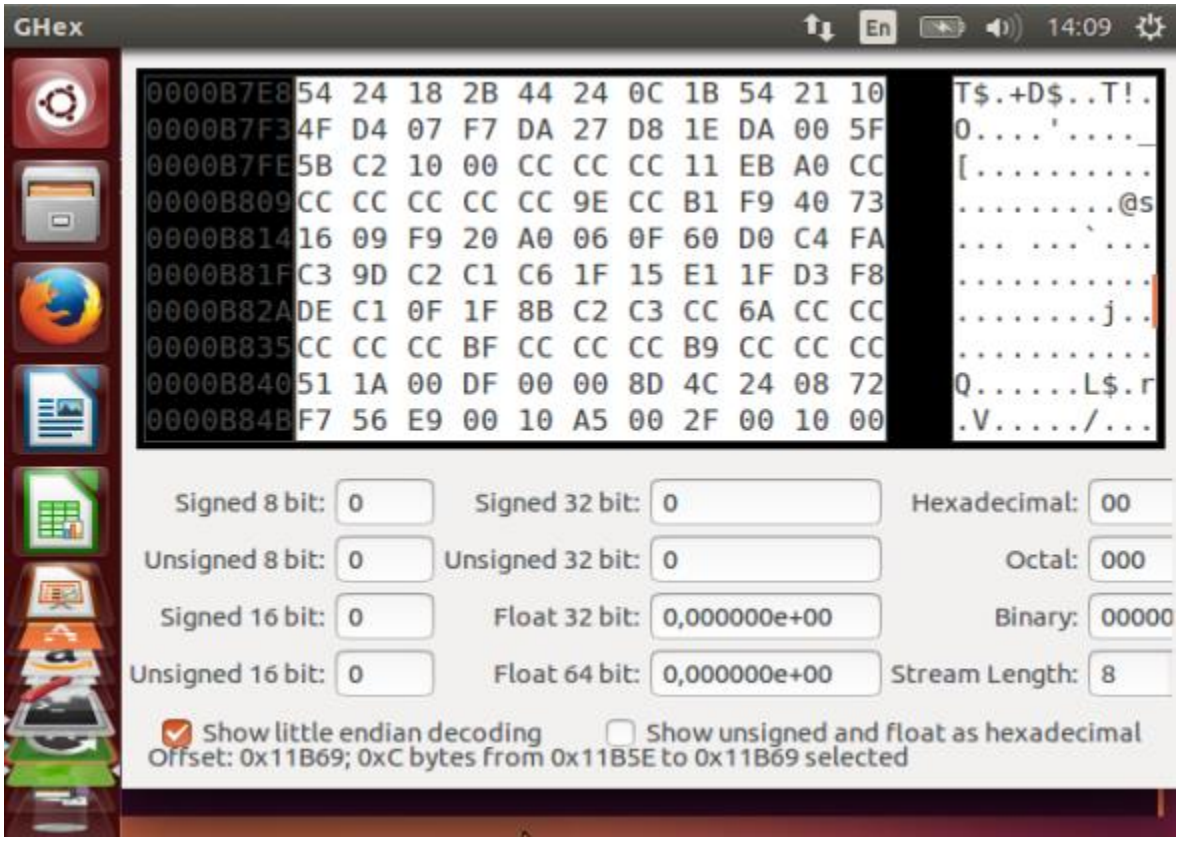
Exploit adalah sebuah kode yang menyerang keamanan_komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan..



Gambar.1 langkah penyerangan dan teknik penyerangan

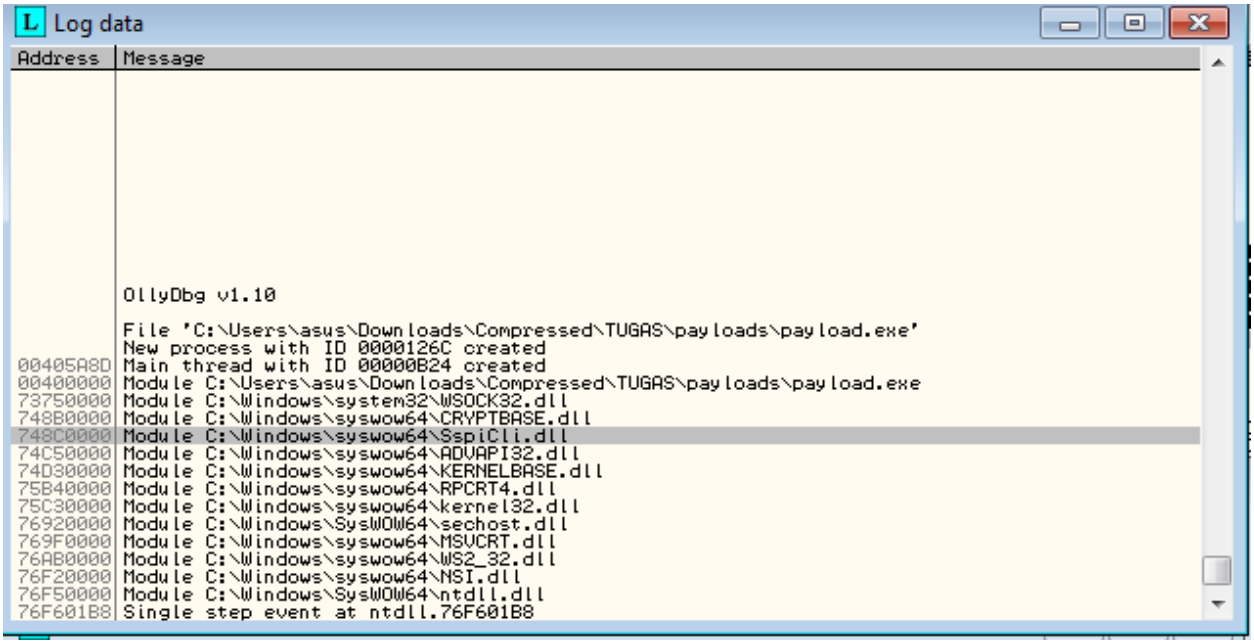
Ada beberapa metode untuk mengklasifikasi exploit. Yang paling umum adalah dengan melihat cara exploit membuat kontak dengan perangkat lunak yang rentan. Remote exploit (eksploit jarak jauh) bekerja melalui jaringan dan mengeksploitasi celah keamanan tanpa adanya akses terlebih dahulu ke sistem korban. Local exploit (eksploit lokal) mengharuskan adanya akses terlebih dahulu ke sistem yang rentan dan biasanya meningkatkan keleluasaan orang yang menjalankan exploit melebihi yang diberikan oleh administrator sistem. Exploit yang menyerang aplikasi klien juga ada, biasanya terdiri dari server-server yang dimodifikasi yang mengirimkan exploit jika diakses dengan aplikasi klien. Exploit yang menyerang aplikasi klien juga mungkin memerlukan beberapa interaksi dengan pengguna, dengan demikian dapat digunakan dalam kombinasi dengan metode social engineering. Ini adalah cara hacker masuk ke komputer dan situs web untuk mencuri data.

ANALISA PROGRAM PAYLOAD DENGAN GHEX



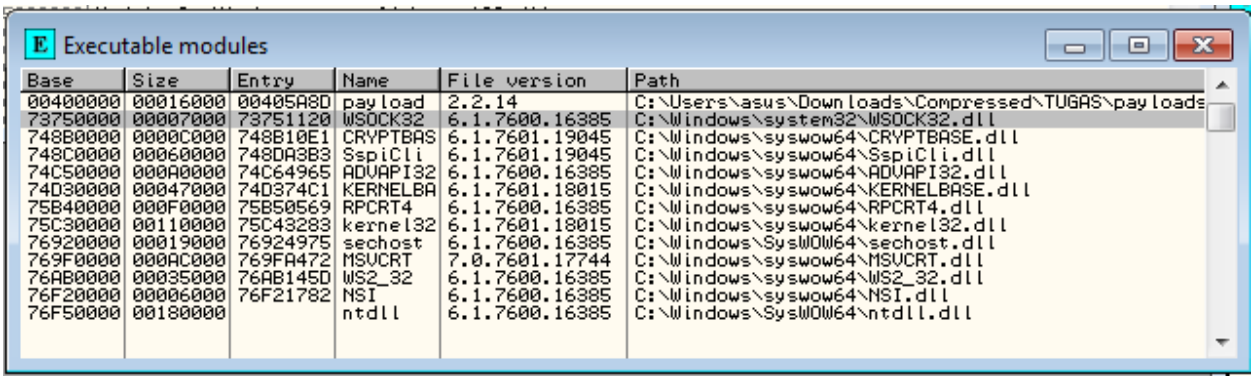
Gambar 2. Analisa payload dengan Ghex

ANALISA PROGRAM PAYLOAD DENGAN Olly Dbg

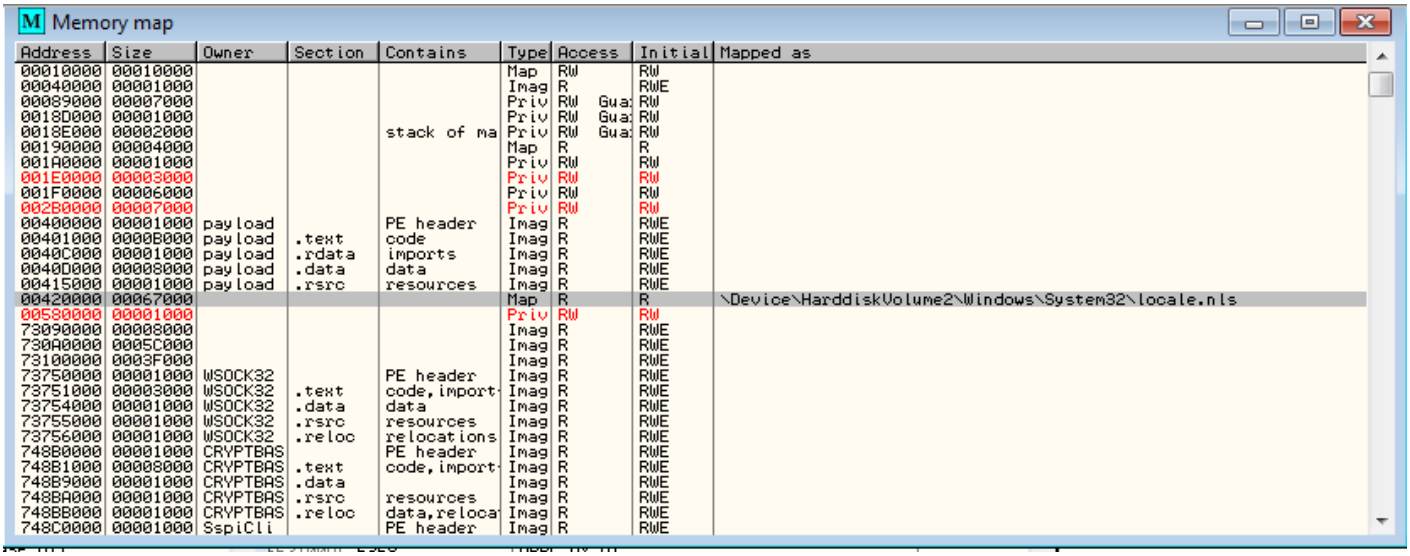


Gambar 3. Tabel log data dari program payload

Dari gambar di atas diketahui bahwa program tersebut akan menyerang pada program file di system32 dan syswow64 pada komputer target. Program payload akan mengirim data melalui jalur socket yang terdapat di dalam program payload yang akan di tunjukan pada attacker dengan protocol dan port ada komuniksi socketnya.

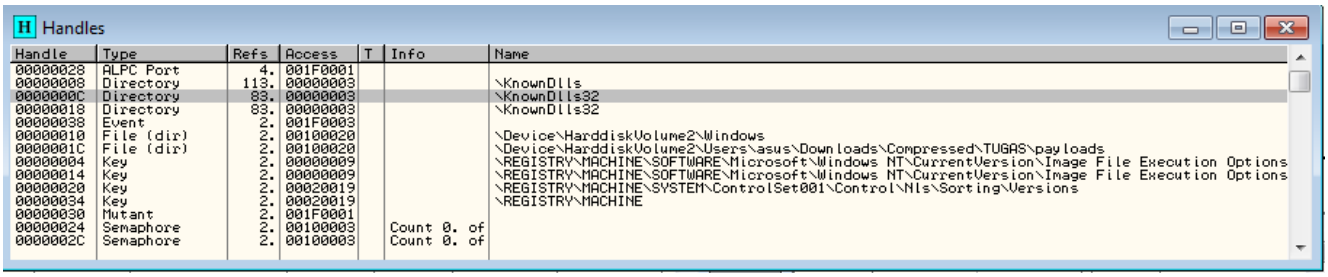


Gambar 4. Tabel modul/program file yang di serang oleh program payload



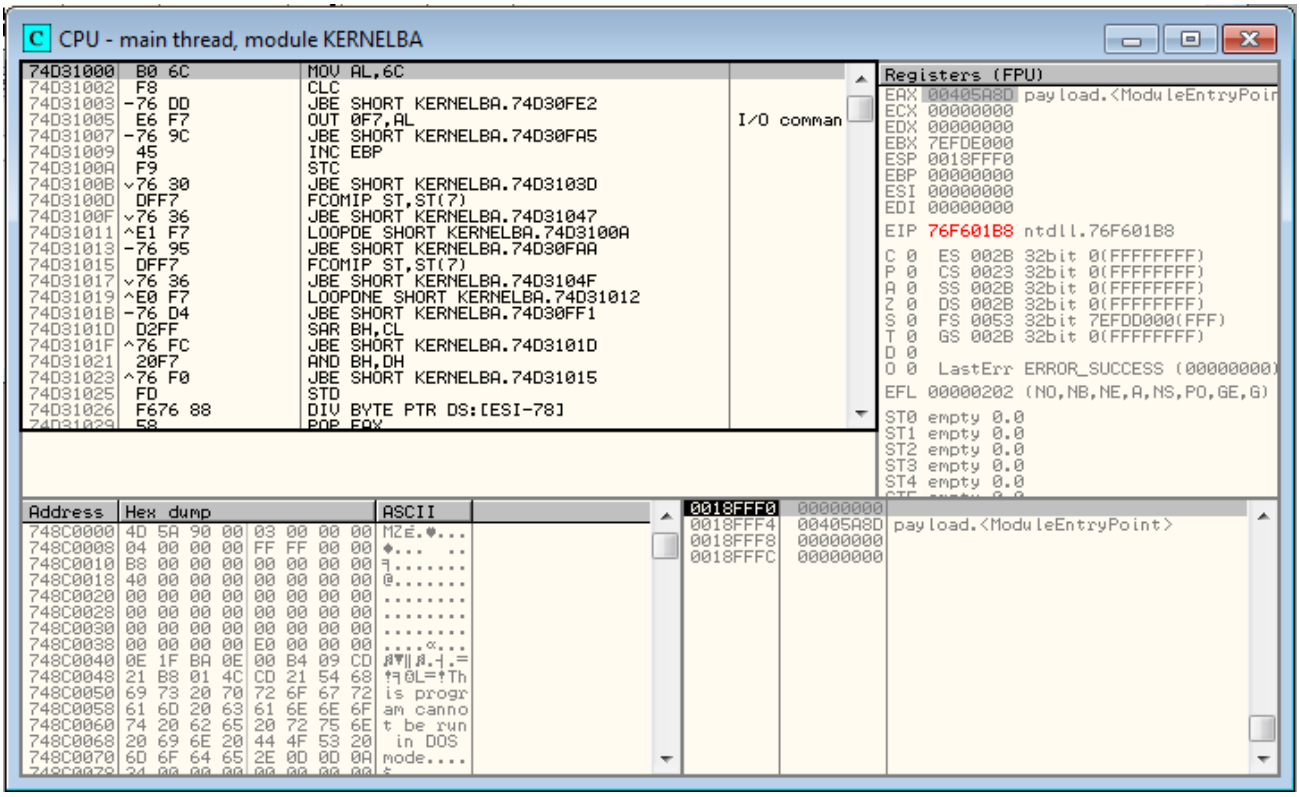
Gambar 4. Tabel peta memori yang di serang oleh program payload

Dalam tabel tersebut terdapat file yang yg diubah oleh payload yang terdapat didalam module sehingga maka akan berubah pada contain dan access pada file tersebut.



Gambar 5. Tabel handle

Terdapat alamat yang di handle oleh program payload ketika sudah terinstall di komputer target.



Gambar 6. Tabel intruksi/main thread

Dalam mengyerang module pada target payload akan melakukan inturksi program untuk mengeksekusi module file yang terdapat di target. Intruksi program dapat di lihat di gambar 6, pada gambar di atas juga terdapat hasil dari hex dump dan dapat dilihat register yang menjadi target oleh program payload.