

**TUGAS KEAMANAN JARINGAN KOMPUTER  
EXPLOIT**

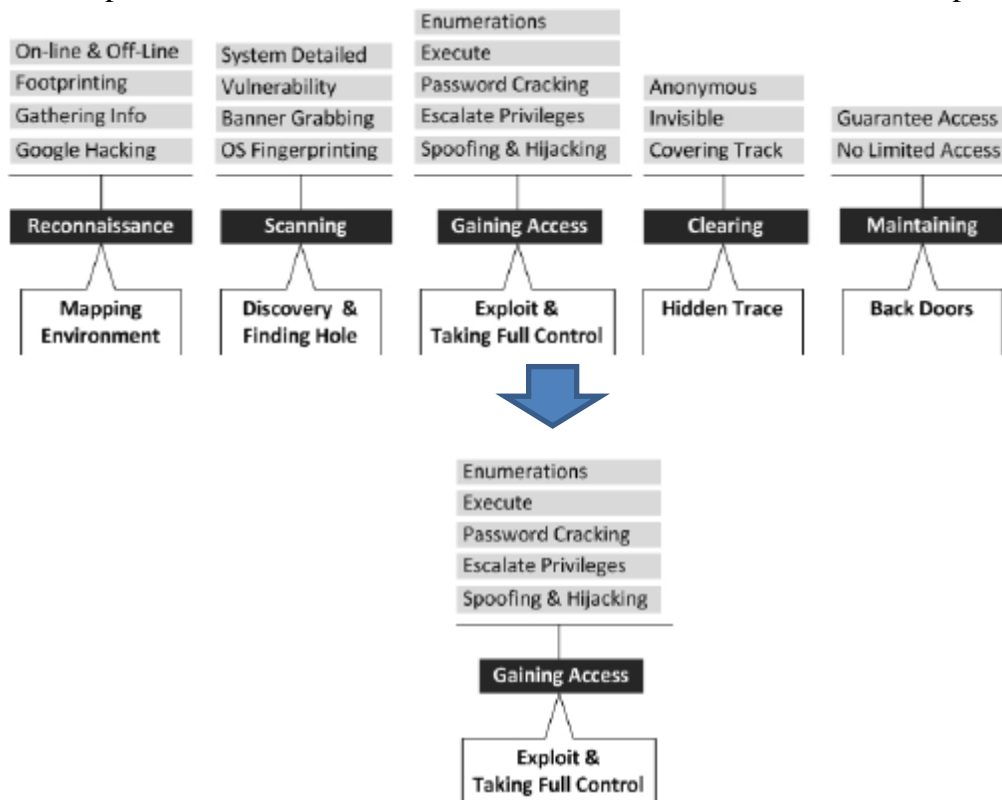


**NAMA: EDI SUKRISNO  
NIM: 0901181320043**

**UNIVERSITAS SRIWIJAYA  
FAKULTAS ILMU KOMPUTER  
JURUSAN SISTEM KOMPUTER  
2017**

# Exploit

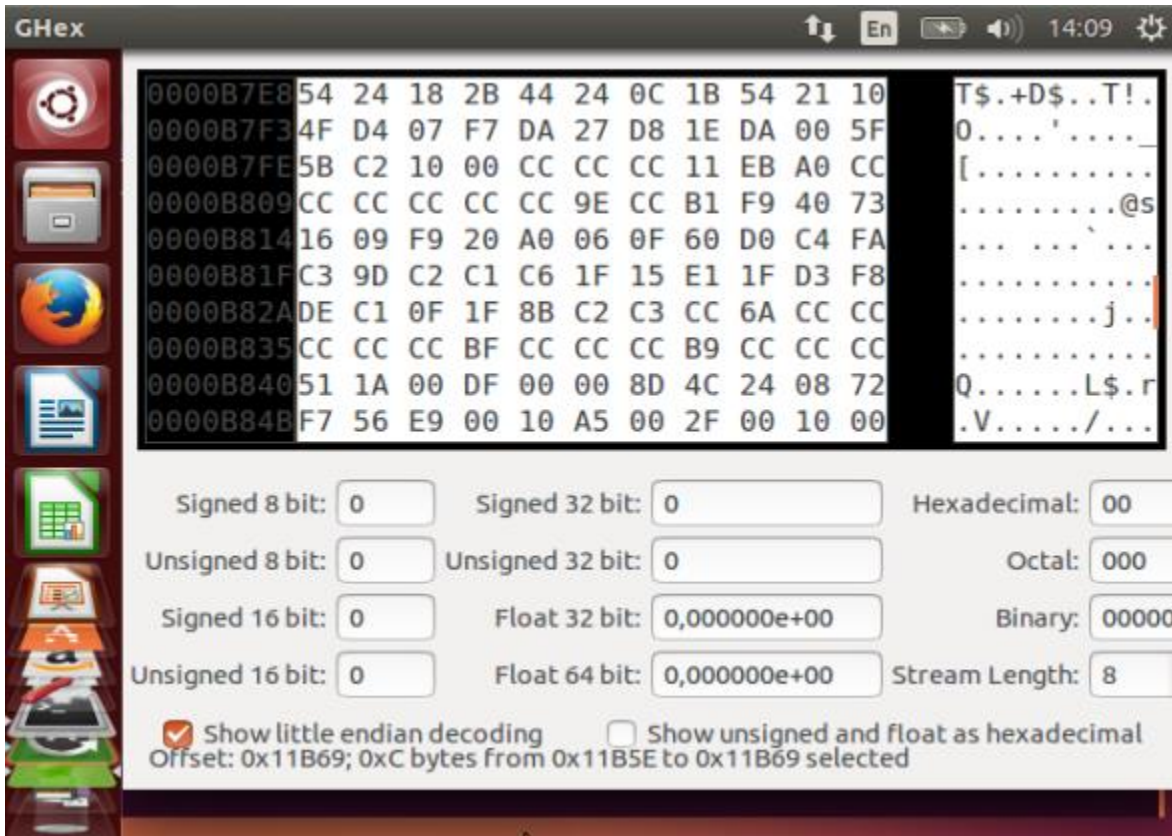
Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penetrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) 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

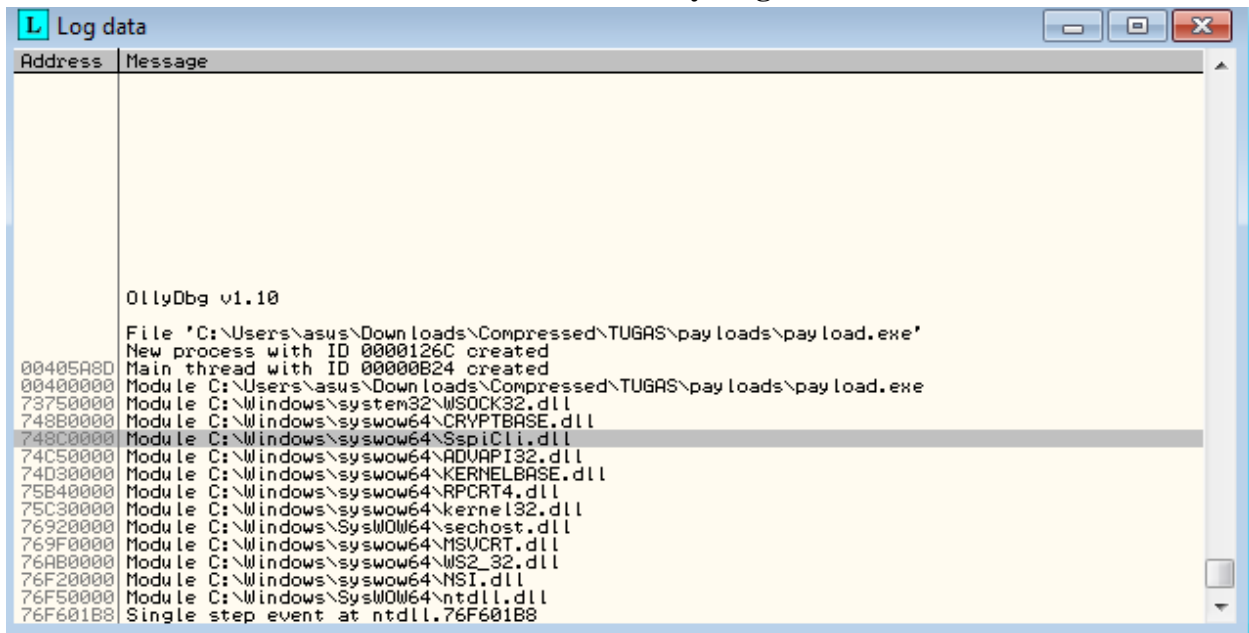
Ada beberapa metode untuk mengklasifikasi exploit. Yang paling umum adalah dengan melihat cara exploit membuat kontak dengan perangkat lunak yang rentan. Remote exploit (eksploit jarak jauh) bekerja melalui jaringan dan mengeksploitasi celah keamanan tanpa adanya akses terlebih dahulu ke sistem korban. 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 komunikasi socketnya.

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A80	payload	2.2.14	C:\Users\asus\Downloads\Compressed\TUGAS\payloads
73750000	00007000	73751120	WSOCK32	6.1.7600.16385	C:\Windows\system32\WSOCK32.dll
748B0000	0000C000	748B10E1	CRYPTBASE	6.1.7601.19045	C:\Windows\syswow64\CRYPTBASE.dll
748C0000	00006000	748DA3B3	SspiCli	6.1.7601.19045	C:\Windows\syswow64\SspiCli.dll
74C50000	000A0000	74C64965	ADVAPI32	6.1.7600.16385	C:\Windows\syswow64\ADVAPI32.dll
74D30000	00047000	74D374C1	KERNELBA	6.1.7601.18015	C:\Windows\syswow64\KERNELBASE.dll
75B40000	000F0000	75B50569	RPCRT4	6.1.7600.16385	C:\Windows\syswow64\RPCRT4.dll
75C30000	00110000	75C43283	kernel32	6.1.7601.18015	C:\Windows\syswow64\kernel32.dll
76920000	00019000	76924975	sechost	6.1.7600.16385	C:\Windows\SystemOW64\sechost.dll
769F0000	000AC000	769FA472	MSUCRT	7.0.7601.17744	C:\Windows\syswow64\MSUCRT.dll
76AB0000	00035000	76AB145D	WS2_32	6.1.7600.16385	C:\Windows\syswow64\WS2_32.dll
76F20000	00006000	76F21782	NSI	6.1.7600.16385	C:\Windows\syswow64\NSI.dll
76F50000	00180000		ntdll	6.1.7600.16385	C:\Windows\SystemOW64\ntdll.dll

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

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00040000	00001000				Image	R	RWE	
00089000	00007000				Priv	RW	Gua: RW	
00180000	00001000				Priv	RW	Gua: RW	
0018E000	00002000			stack of ma	Priv	RW	Gua: RW	
00190000	00004000				Map	R	R	
001A0000	00001000				Priv	RW	RW	
001E0000	00003000				Priv	RW	RW	
001F0000	00006000				Priv	RW	RW	
00250000	00007000				Image	RW	RW	
00400000	00001000	payload		PE header	Image	R	RWE	
00401000	0000B000	payload	.text	code	Image	R	RWE	
0040C000	00001000	payload	.rdata	imports	Image	R	RWE	
0040D000	00008000	payload	.data	data	Image	R	RWE	
00415000	00001000	payload	.rsrc	resources	Image	R	RWE	
00420000	00007000				Map	R	R	\\Device\HarddiskVolume2\Windows\System32\locale.nls
00580000	00001000				Priv	RW	RW	
73090000	00008000				Image	R	RWE	
730A0000	0000C000				Image	R	RWE	
73100000	00003000				Image	R	RWE	
73750000	00001000	WSOCK32		PE header	Image	R	RWE	
73751000	00003000	WSOCK32	.text	code, import	Image	R	RWE	
73754000	00001000	WSOCK32	.data	data	Image	R	RWE	
73755000	00001000	WSOCK32	.rsrc	resources	Image	R	RWE	
73756000	00001000	WSOCK32	.reloc	relocations	Image	R	RWE	
748B0000	00001000	CRYPTBASE		PE header	Image	R	RWE	
748B1000	00008000	CRYPTBASE	.text	code, import	Image	R	RWE	
748B9000	00001000	CRYPTBASE	.data	data	Image	R	RWE	
748BA000	00001000	CRYPTBASE	.rsrc	resources	Image	R	RWE	
748BB000	00001000	CRYPTBASE	.reloc	data, reloca	Image	R	RWE	
748C0000	00001000	SspiCli		PE header	Image	R	RWE	

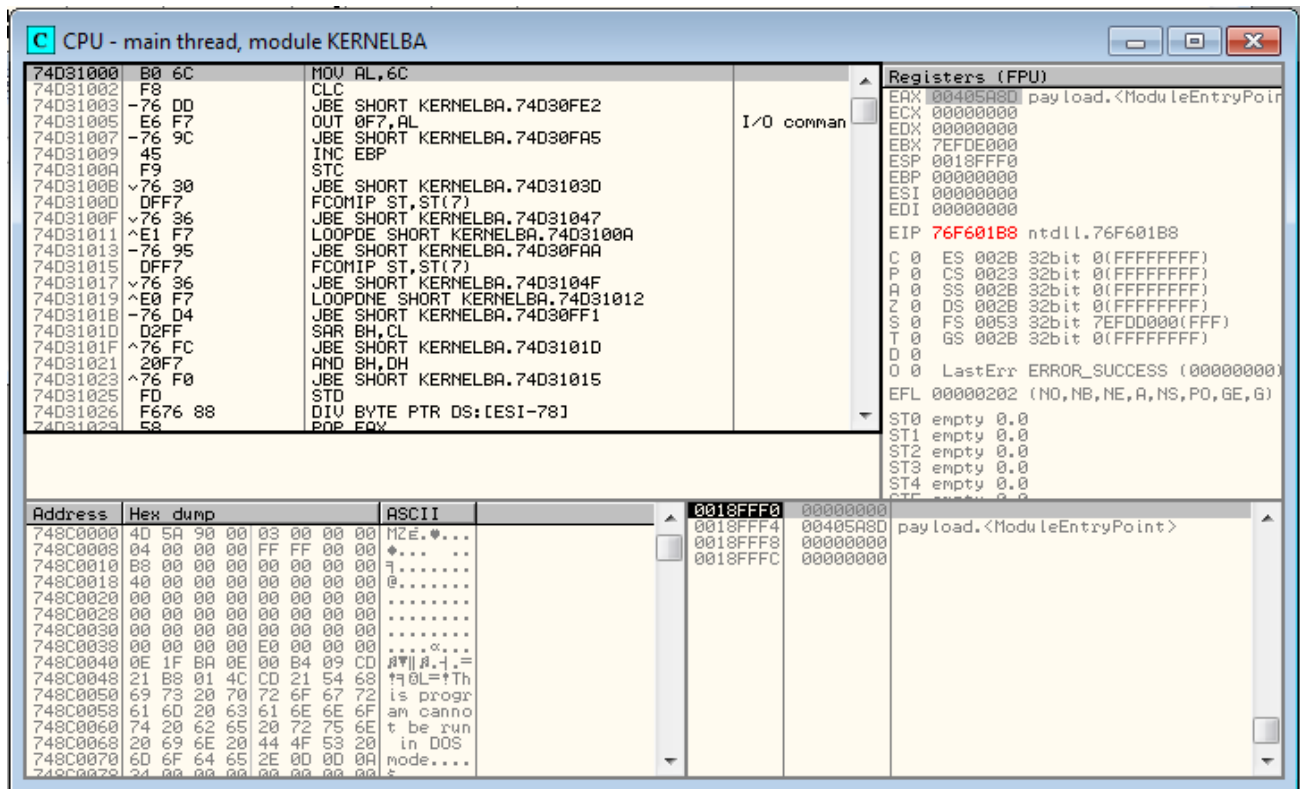
Gambar 4. Tabel peta memori yang di serang oleh program payload

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.

Handle	Type	Refs	Access	T	Info	Name
00000028	ALPC Port	4	001F0001			
00000003	Directory	113	00000003			\\KnownDlls
0000000C	Directory	83	00000003			\\KnownDlls32
00000013	Directory	83	00000003			\\KnownDlls32
00000038	Event	2	001F0003			
00000010	File (dir)	2	00100020			\\Device\HarddiskVolume2\Windows
0000001C	File (dir)	2	00100020			\\Device\HarddiskVolume2\Users\asus\Downloads\Compressed\TUGAS\payloads
00000004	Key	2	00000009			\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
00000014	Key	2	00000009			\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
00000020	Key	2	00020019			\\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00000034	Key	2	00020019			\\REGISTRY\MACHINE
00000030	Mutant	2	001F0001			
00000024	Semaphore	2	00100003		Count 0. of	
0000002C	Semaphore	2	00100003		Count 0. of	

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 menyerang module pada target payload akan melakukan intruksi 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.