Tugas Mata Kuliah

KEAMANAN JARINGAN KOMPUTER



Nama : Faris Abdul Aziz Nim : 09011181320020

Jurusan Sistem Komputer

Fakultas Ilmu Komputer Universitas Sriwijaya

2017

MALWARE

Malware adalah adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari software.

Tools yang digunakan adalah:

- 1. Strings
- 2. GHex
- 3. Ollydbg
- 4. Hexdump

Dengan file target:

- 1. Payload
- 2. Payload2

Pertama menggunakan perintah strings pada payload, string sendiri berguna untuk mengurutkan karakter, mencari karakter, memilih karakter yang ingin ditampilkan. Dan dapat dilihat perintah string pada gambar 1.1 dibawah.

LOG: header received: apr_socket_recv //P //P //P //P //P //P //P //	faris@farismr ~/Documents/TUGAS/payloads \$ strings payload.exe [
LGG: header received: apr socket recv Licensed to The Apache Software Foundation, http://www.zeustech.net/dbr> This is ApacheBench, Version %s ciskLiks&git SRevision: 655654 \$ Licensed to The Apache Software Foundation, http://www.zeustech.net/ This is ApacheBench, Version %s ciskLiks&git 2.3 seRevision: 655654 \$ 2.3 seRevision: 655654 \$ 6.6 If the apache Software Foundation (this message) 7. Don't exit on socket receive errors. 6. e filename Output COSV file with percentages served 9. difference estimators and maintigs. 7. Do not show confidence estimators and maintigs. 7. do not show confidence estimators and maintigs. 7. V Print Version number and exit 7. Add Basic MW Authentication, the attributes 7. attribute 7. Add Basic MW Authentication, the attributes 7. Add Absirser Verset Lines. (repeatable) 7. Hattribute 7. Add Absirser Verset Lines. (repeatable) 7. Attributes 7. Just Add Absirser Verset Lines. (repeatable) 7. Add Absirser Verset Lines. (repeatable) 7. Just Add Absirser Verset Lines. (repeatable) 7. Add Absirser Verset Lines. (repeatable) 7. Attributes 7. Just Add Cookie, eg. 'Apache-1234, (repeatable) 7. Just Add Cookie, eg. 'Apache-1234, (repeatable) 7. Just Add Absirser Verset Lines. (repeatable) 7. Just Add Cookie, eg. 'Apache-1234, (repeatable) 7. Just Add Cookie, eg. 'Apache-1234, (repeatable) 7. Just Add Cookie, eg. 'A						
apr Jocket recv <pre> cyp: Licensed to The Apache Software Foundation, http://www.apache.org/ Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://wwww.apache.org/ Copyright 1996 Adam Twiss, Technology Ltd, ht</pre>	LOG: header receive	d: name Help				
<pre>Victures 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 d-Soltix#s&gtv:/i-vers</pre> SRevision: 655654 \$ 2.3 <akevision: \$="" 3.3="" 4.4="" 655654="" <akevision:="" hit="" percentages="" served<="" th="" use=""><th>apr_socket_recv</th><th></th><th></th><th></th><th></th></akevision:>	apr_socket_recv					
<pre>Copyright 1996 Adam Twiss. Zeus Technology Ltd, http://www.zeustech.net/ This is ApacheBench, Version %s <lobal and="" sta<="" status="" th="" the=""><th colspan="3"></th><th></th><th>'白'음'문 유 문 두</th></lobal></pre>					'白'음'문 유 문 두	
This is ApacheBench, Version Ns <isalt;%sgt;~ j=""> Breision: 655654 \$ Licensed to The Apache Software Foundation, http://www.zeustech.net/ This is ApacheBench, Version Ns <isalt,%sgt;~ j=""> Disply usage information (this message) Don't exit on socket receive errors. - re filename Output CSV file with percentages served of filename Output CSV file with percentages served to show confidence estimators and warnings. - d Do not show percentlies served table. - k Use HTTP KeepAlue feature - Y Print version number and exit - x proxy:port Proxyserver and port number to use - a tattribute - A dtribute Add Basic Proxy Authentication, the attributes - a tattribute Add Basic Proxy Authentication, the attributes - A attribute Add Basic Proxy Authentication, the attributes - A attribute String to insert as to d'rethoutes - y attributes String to insert as to d'rethoutes - y extributes String to insert as to d'rethoutes - y werbosity How wich form your lencoded' - y uputfile File containing to print - w Print our results in HTML tables - y extributes String to insert as the attributes - y outprint our results in HTML tables - y verbosity How wich rows form your lencoded' - y outprint our results in HTML tables - y outprint our results in HTML tables - y verbosity How much rows form your lencoded' - y outprint outprint point number also to set -T</isalt,%sgt;~></isalt;%sgt;~>	Convright 1996 Adam Twiss, Zeus Technology Lid, http://www.apache.org/sb/s					
<pre>SRevision: 655654 \$ Licensed to The Apache Software Foundation, http://www.zeustech.net/ This is ApacheBench, Version %s 2.3 <\$Revision: 655654 \$></pre>	This is ApacheBench. Version % <i><:%s&at:/i> </i>					
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 \$> - Don't exit on socket receive errors. - e filename Output CSV file With percentages served - g filename Output CSV file With percentages served - g filename Output CSV file With percentages served - d Do not show confidence estimators and warnings. - d 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 - P attribute Add Basic Proxy Authentication, the attributes are a colon separated username and password. - A attribute Add Basic Wuthentication, the attributes Inserted after all normal header lines. (repeatable) - t Add cookie, eg. 'Apache=1234. (repeatable) - attributes String to insert as traitributes - y attributes String to insert as traitributes - w werbosity How much troubleshooting info to print Default is 'text/plain' - apulcialiny.*ww-form-urlencoded' - T content-type Content.type header for POSTing, eg. - uputfile File containing data to PUI.	\$Revision: 655654 \$					
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/ This is ApacheBench, Version %5 2.3 <8Revision: 655654 \$> - n Don't exit on socket receive errors. - of Don't exit on socket receive errors. - of filename Output collected data to gnuplot format file. - of 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 WW Authentication, the attributes Inserted after all normal header lines, (repeatable) + attribute Add cookie, eg. 'Accept-Encoding: gzip' - C attribute String to insert as the attributes - y attributes String to insert as the attributes - a thributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - a thributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - u w Print our results in HTML tables - v verbosity How much troubleshooting info to print Default is 'text/plain' - application/x-ww-form-unlencoded' - r content-type Content-type Moder for POSTing, eg. - up uptile File containing data to PUT. Remember also to set -T	Licensed to The Apa	che Software Foundation, http://www.apache.org/			davie o div	
<pre>Ints is Apachebench, version %s 2.3 -sRevision: 655564 \$> - 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 supplot 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 - P attribute Add Basic Proxy Authentication, the attributes are a colon separated username and password A attribute Add Basic WW Authentication, the attributes Inserted after all normal header lines. (repeatable) - attribute Add cookie, eg. 'Apache=1234. (repeatable) - attributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - i Use HEAD instead of GET - w Print versioning info to print Default is 'text/plain' - application/x-ww-form-urlencoded' - T content-type Content-type Reder for POSTing, eg u putfle File containing data to PUT. Remember also to set -T - Use Add Application/x-Werform-urlencoded' - T content-type Content-</pre>	Copyright 1996 Adam	Twiss, Zeus Technology Ltd, http://www.zeustech.net/			and the second second	
<pre>-h Display usage information (this message) -r Don't exit on socket receive errorse filename Output CSV file with percentages served g filename Output cSV file with percentages served -s Do not show confidence estimators and warningsd Do not show percentiles served tablek Use HTTP KeepAlive feature -V Print version number and exit -x proxy:port Proxyserver and port number to use -A attribute Add Basic MW Authentication, the attributes are a colon separated username and passwordA attribute Add Cookie, eg. 'Apache=1234, (repeatable) +H attribute Add cookie, eg. 'Apache=1234, (repeatable) -z attributes String to insert as the attributes -x attributes S</pre>	7 3 stRevision: 655	, VERSION %5				
<pre>-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 percentiles served table. -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 WW Authentication, the attributes Inserted after all normal header line, (repeatable) -H attribute Add cookie, eg. 'Apache=1234. (repeatable) -2 attributes String to insert as the attributes -y attributes String to insert as the attributes -y attributes String to insert as the attributes -y attributes String to insert as the attributes -i Use HEAD instead of GET -w Print our results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application'x-ww-form-urlencoded' -T content-type Content-type Hoader for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T</pre>	-h	Display usage information (this message)			and the second	
 e filename Output CSV file with percentages served g filename Output collected data to gnuplot format file. 5 Do not show confidence estimators and warnings. d Do not show percentiles served table. k Use HTP KeepAlive feature V Print version number and exit A dt Basic Proxy Authentication, the attributes a c colon separated username and password. A attribute Add Basic WW Authentication, the attributes Inserted after all normal header lines. (repeatable) H attribute Add cookie, eg. 'Apache=1234. (repeatable) - attributes String to insert as the attributes y attributes String to insert as the attributes - y attributes String to insert as the attributes - y attributes String to insert as the attributes - i Use HEAD instead of GET - w Print out results in HTML tables - v verbosity How much troubleshooting info to print Default is 'text/plain' - application/x-ww-form-urlencoded' - T content-type Content-type How The Member also to set -T 	- r 2	Don't exit on socket receive errors.			standardiene server	
<pre></pre>	-e filename	Output CSV file with percentages served				
 S Do not show percentiles served table. -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 WW Authentication, the attributes Inserted after all normal header lines. (repeatable) -H attribute Add cookie, eg. 'Apache=1234. (repeatable) -c attributes String to insert as the attributes -y attributes String to insert as trattributes -i Use HEAD instead of GET -w Print our results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application', ew.'Form-urlencoded' -T content-type Content-type Hoader for POSTing, eg. 	-g filename	Output collected data to gnuplot format file.			A REAL PROPERTY AND A REAL PROPERTY AND A	
 -d Do not show percentiles served table. -k Use HTP KeepAlive feature -V Print version number and exit -> Pattribute -> Add Basic Proxy Authentication, the attributes -> are a colon separated username and password. -> A attribute -> Add Basic WW Authentication, the attributes -> are a colon separated username and password. -> A attribute -> Add Arbitrary header lines. (repeatable) -> H attribute -> Add cookie, eg. 'Apache=1234. (repeatable) -> c attributes -> String to insert as to rh attributes -> y attributes -> string to insert as to rh attributes -> verbosity +> werbosity +> werbosity -> verbosity +> tortype Content-type Roader for POSTing, eg. -> up utfile -> File containing data to PUT. Remember also to set -T 	-S	Do not show confidence estimators and warnings.				
 N use HIP KeepAlve 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 NWW Authentication, the attributes Inserted after all normal header lines. (repeatable) H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip' C attribute S tring to insert as td or th attributes y attributes String to insert as td or th attributes y attributes String to insert as td attributes use HEAD instead of GET w Print out results in HTML tables v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' T content-type Content-type Reader for POSTing, eg. 	-d	Do not show percentiles served table.				
 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 WW Authentication, the attributes 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) - 2 attributes String to insert as tor thattributes - y attributes String to insert as trattributes - i Use HEAD instead of GET - w Print out results in HTML tables - v verbosity How much troubleshooting info to print Default is 'text/plain' - aplication/x-ww-form-urlencoded' - T content-type Content-type Hoader for POSTing, eg. 	- K - V	Dise nilp Reepairve reduire			Rossid Laksus	
<pre>-P attribute Add Basic Proxy Authentication, the attributes are a colon separated username and password. -A attribute Add Basic WW Authentication, the attributes Inserted after all normal header lines. (repeatable) -H attribute Add crokie, eg. 'Acapache=1234. (repeatable) -c attributes Atring to insert as the rot hattributes -y attributes String to insert as the attributes -y attributes String to insert as the attributes -i Use HEAD instead of GET -w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-ww-form-urlencoded' -T content-type Content-type header for POSTing, eg.</pre>	-X proxy:port	Proxyserver and nort number to use			sector for an interview of the	
are a colon separated username and password. -A attribute Add Basic WWW Authentication, the attributes Inserted after all normal header lines. (repeatable) +H attribute Add Arbitrary header lines, (repeatable) -t attribute Add cookie, eg. 'Apache=1234. (repeatable) -z attributes String to insert as td or th attributes -z attributes String to insert as td or th attributes -z attributes String to insert as table attributes -z optication/x-www-form-urlencoded' -z optication/x-www-form-UT. Remember also to set -T	-P attribute	Add Basic Proxy Authentication, the attributes			(The set) The strength The rest.	
- A attribute Add Basic WWW Authentication, the attributes Inserted after all normal header lines, (repeatable) -H attribute Add cookie, eg. 'Apache=1234. (repeatable) -2 attributes String to insert as tor tha attributes -y attributes String to insert as tor thattributes -x attributes String to insert as table attributes -x attributes Is instad of GET -w Print our results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application'x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T	Here I betwices	are a colon separated username and password.			Fathimaty Asy-synthetic	
Inserted after all normal header lines. (repeatable) H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip' - C attributes Add cookie, eg. 'Acpache=1234. (repeatable) - 2 attributes String to insert as that that the second se	-A attribute	Add Basic WWW Authentication, the attributes			and a support to be sublet to	
 H attribute Add Arbitrary header Line, eg. 'Accept-Encoding: g2ip' C attributes Add cookie, eg. 'Apache=1234. (repeatable) -z attributes String to insert as td or th attributes -y attributes String to insert as table attributes -y attributes String to insert as table attributes -i Use HEAD instead of GET -w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' -application/x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T 		Inserted after all normal header lines. (repeatable)			Linetite	
 attributes Add Cooke, eg. Apathe-1234. (repeatable) attributes String to insert as the attributes y attributes String to insert as table attributes attributes String to insert as table attributes use HEAD instead of GET w Print out results in HTML tables v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' T content-type Content-type header for POSTing, eg. up utfile File containing data to PUT. Remember also to set -T 	-H attribute	Add Arbitrary header line, eg. 'Accept-Encoding: gzip'			Depe Munanimus	
<pre>-y attributes String to insert as tr attributes -x attributes String to insert as tr attributes -i Use HEAD instead of GET -w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T</pre>	-c attributes	String to incert as the or th attributes				
 -x attributes String to insert as table attributes i Use HEAD instead of GET -w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T 	-v attributes	String to insert as tr attributes			B replace beaution as	
-i Use HEAD instead of GET -w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application'x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T	-x attributes	String to insert as table attributes				
-w Print out results in HTML tables -v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T	Finatson	Use HEAD instead of GET			Place Report areas	
-v verbosity How much troubleshooting info to print Default is 'text/plain' 'application/x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T	-W	Print out results in HTML tables				
uerault 15 'text/plain' 'application'x-www-form-urlencoded' -T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T	-v verbosity	How much troubleshooting info to print			American American	
-T content-type Content-type header for POSTing, eg. -u putfile File containing data to PUT. Remember also to set -T		perault 1s 'text/plain'				
- u putfile File containing data to PUT. Remeber also to set -T	-T content-type	Content-type header for POSTing eq			The Loss Diministration of	
	-u putfile	File containing data to PUT. Remember also to set -T			A CONTRACTOR OF A CONTRACTOR O	
-p postfile File containing data to POST. Remember also to set -T	-p postfile	File containing data to POST. Remember also to set -T			RENTAR LANNING (25)	
-b windowsize Size of TCP send/receive buffer, in bytes	-b windowsize	Size of TCP send/receive buffer, in bytes				
-t timeLimit Seconds to max, wait for responses	-t timelimit	Seconds to max. wait for responses			and the American American -	
- C CONCULTENCY NUMber of multiple requests to make	-c concurrency	Number of multiple requests to make			A Real Provide State	
	Options are:	Number of requests to perform			CA Dan Bunda	



Gambar 1.1. String pada payload

Terlihat pada perintah string pada gambar 1.1, terdapat banyak karakter yang dimiliki oleh file playload, dan kita dapat melihat dan memilih karakter apa saja yang ada didalem file payload diatas.

Lalu dilanjutkan dengan melakukan perintah string ke file ke dua, yaitu payload2. Dan dapat dilihat pada gambar 1.2 dibawah.



Gambar 1.2. Strings pada payload2

Terlihat tulisan user attacker Ganteng1, menurut saya, file payload2 ini telah dicrack(diserang) dan diberikan malware, sehingga membuat file payload2 menjadi corrupt.

Setelah itu lakukan perintah GHex pada kedua file payload dan payload2 untuk melihat keamanan pada kedua file tersebut. Dapat dilihat GHex pada payload dan payload2 pada gambar 1.3 dibawah.

payload.exe - GHex - + ×							
File Edit View Windows Help							
000000004D 5A 90 00 03 00 00 00 04 00 0	0 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00	00 00 00 00 MZ					
0000003F00 00 0F 1F BA 0F 00 B4 09 CD 2	1 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61	6D 20 63 61					
0000005D6E 6E 6F 74 20 62 65 20 72 75 6	E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A	24 00 00 00 nnot be run in DOS mode\$					
0000007C00 00 00 00 93 38 F0 D6 D7 59 9	E 85 D7 59 9E 85 D7 59 9E 85 AC 45 92 85 D3 59 9E	85 54 45 908YYYEYTE.					
0000009B85 DE 59 9E 85 B8 46 94 85 DC 5	9 9E 85 B8 46 9A 85 D4 59 9E 85 D7 59 9F 85 1E 59	9E 85 54 51YFYFYYYYTQ					
000000BAC3 85 DF 59 9E 85 83 7A AE 85 F	F 59 9E 85 10 5F 98 85 D6 59 9E 85 52 69 63 68 D7	59 9E 85 00YzYYRich.Y					
	0 00 00 00 00 50 45 00 00 4C 01 04 00 47 71 D6 49 6 00 00 80 00 00 00 00 00 00 00 00 00 00	00 00 00 00PELGq.I					
	0 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00					
0000013600 00 00 60 01 00 00 10 00 00 0	0 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00	00 10 00 00`					
0000015510 00 00 00 00 00 00 10 00 00 0	0 00 00 00 00 00 00 00 00 6C C7 00 00 78 00 00 00	00 50 01 00P					
00000174C8 07 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 00 00 0	00 E0 C1 00					
	0 00 00 00 00 00 00 00 00 00 00 00 00 0						
	0 00 00 00 00 C0 00 00 E0 01 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00					
000001F000 B0 00 00 00 10 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00 00 20 00 00	61 74 61 00					
0000020F00 E6 0F 00 00 00 C0 00 00 1	0 00 00 00 C0 00 00 00 00 00 00 00 00 00	00 00 40 00@.					
0000022E00 40 2E 64 61 74 61 00 00 00 5	C 70 00 00 00 D0 00 00 00 40 00 00 00 D0 00 00 00	00 00 00 00 .@.data\p@@.					
0000024D00 00 00 00 00 00 00 40 00 00 C	0 2E 72 73 72 63 00 00 00 C8 07 00 00 00 50 01 00	00 10 00 00@rsrcP					
	0 00 00 00 00 00 40 00 00 40 00 00 00 00	00 00 00 00					
Signed 8 bit: 77	Signed 32 bit: 9460301	Hexadecimal: 4D					
Unsigned 8 bit: 77	Unsigned 32 bit: 9460301	Octal: 115					
Signed 16 bit: 23117	Float 32 bit: 1,325671e-38	Binary: 01001101					
Unsigned 16 bit: 23117	Float 64 bit: 6,370661e-314	Stream Length: 8 – +					
🖸 Show little endian decodin	Show unsigned and float as hexadecimal						
Offset: 0x0							

Gambar 1.3. GHex pada payload

Pada gambar 1.3 terlihat kode encrypt pada file payload. Pada GHex payload terdapat banyak kode encrypt di dalamnya, karena pada file payload memiliki banyak karakter. Lalu kita GHex juga file payload2, dapat dilihat pada gambar 1.4 dibawah.

payload2.exe - GHex – + ×							
File Edit View Windows Help							
00000000 FC E 8 2 00 00 60 89 E5 31 C0 64 88 50 30 88 52 0C 8 00000001F3C 61 7C 02 2C 20 C1 CF 00 01 7 E2 F2 52 57 78 52 10 8 0000003E59 20 01 3 88 49 18 E3 3A 49 88 34 88 01 D6 68 C 48 85 12 C1 D 06 00 A8 49 18 34 49 88 34 88 01 D6 A1 FF AC D D0 00 A8 A6 A6 D D D D D D D D D D D D D D D D D D D	B 52 14 8B 72 28 0F B7 4A 26 31 FF AC `ld.P0.RRr(J&l B 4A 3C 8B 4C 11 78 E3 48 01 D1 51 8B <al,rw.rj<.l.x.hq.< td=""> 1 CF 0D 01 C7 38 E0 75 F6 03 7D F8 3B <al,rw.rj<.l.x.hq.< td=""> 3 80 04 8B 01 D0 89 44 24 24 5B 5B 61 \$su</al,rw.rj<.l.x.hq.<></al,rw.rj<.l.x.hq.<>						
Signed 8 bit: -4 Signed 32 bi	t: 8579324 Hexadecimal: FC						
Unsigned 8 bit: 252 Unsigned 32 bit	t: 8579324 Octal: 374						
Signed 16 bit: -5892 Float 32 bi	t: 1,202219e-38 Binary: 11111100						
Unsigned 16 bit: 59644 Float 64 bit	t: -1,587866e-263 Stream Length: 8 - +						
Show little endian decoding	Show unsigned and float as hexadecimal						
Offset: 0x0							

Gambar 1.4. GHex pada payload2

Pada gambar 1.4 terlihat sedikit kode encrypt didalamnya, itu dikarenakan file payload2 telah diserang malware dan corrupt. Sehingga karakter pada file payload2 telah hilang.

Selanjutnya dilakukan dengan menggunakan tools ollydbg, untuk ollydbg sendiri tidak dapat membaca file payload2, sehingga ollydbg dilakukan pada file payload saja. Dan dapat dilihat pada gambar 1.5 dibawah.



Gambar 1.5. Ollydbg pada payload

Pada ollydbg gambar 1.5, itu sendiri menu CPU, yang dimana menu CPU itu sudah include pilihan lainnya seperti main thread, module, memory, dan lain-lain. Terdapat juga Hexdump didalamnya, yang dimana hexdump sendiri adalah bilangan heksadesimal dari data computer, dari RAM, atau dari file atau perangkat penyimpanan. Hexdump sendiri direpresentasikan sebagai angka heksadesimal dua digit, yang dimana seperti gambar 1.5 hexdump memiliki 2 angka yang masing-masing dipisahkan oleh kolom putih atau spasi.

Untuk Executable modules sendiri berfungsi untuk mencatat apa saja yang masuk pada ollydbg yang sedang standby saat itu. Dapat dilihat pada kolom executable terdapat apa saja yang masuk

kedalam prosess saat ini, seperti contoh file payload yang terekam oleh executable. Dapat dilihat pada gambar 1.6 dibawah.



Gambar 1.6. Executable Modules