User Guide

LogAnalyzer

Pre-Installation

1. geolite2

   For getting a country information from IP address, we need geolite2

   pip install maxminddb-geolite2

2. tqdm

   tqdm instantly make loops show a smart progress meter

   pip install tqdm

How to use

python ApacheLogAnalyzer.py (log file path)

For example, ‘python ApacheLogAnalyzer.py ./CTF1.log’

Then, you will get following files and directory.

1. SimpleIPList.csv
   - Unique IP address are in lines
2. DetailIPList.csv
   - Unique IP address with country and number of hits are in lines
3. Activity
   - Activity is directory and there are many (unique IP).csv files in Activity. Each csv files have activity which is consist of W3C extended log format fileds per unique IP address.
4. sqli_list.csv
   - It consists of suspicious lines as SQL injection.
5. rfi_list.csv
   - It consists of suspicious lines as Remote File Inclusion.
6. webshell_list.csv
   - It consists of suspicious lines as web shell
7. exception.txt
   - If some line is not matched with W3C extended log format, the line is saved in exception.txt

CSV

1. SimpleIPList.csv

	A
1	75.120.252.187
2	205.123.95.71
3	198.72.2.70
4	78.159.215.111
5	72.240.44.11
6	50.173.44.118
7	207.255.13.114
8	74.36.133.219
9	155.213.224.59
10	64.126.60.130
11	172.12.206.2
12	98.254.49.125
13	173.89.13.41
14	108.44.213.248
15	70.124.238.155

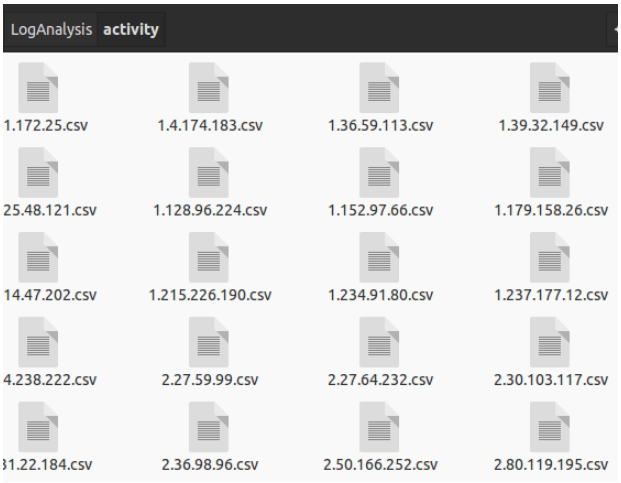
This csv has only client IP address column. And There are unique IP address line by line

2. DetailIPList.csv

7	66.249.91.44	United States	1
8	76.182.20.81	United States	59
9	206.53.110.228	United States	118
10	76.204.3.132	United States	117
11	144.230.63.52	United States	1
12	107.131.198.92	United States	195
13	172.8.129.80	United States	205
14	66.87.72.215	United States	99
15	99.62.90.246	United States	60
16	81.144.138.34	United Kingdom	3
17	108.20.220.189	United States	88
18	64.251.51.194	United States	1
19	74.179.168.220	United States	1
20	172.56.21.193	United States	51
21	67.232.76.19	United States	92
22	70.194.146.103	United States	75
23	199.250.65.70	United States	25
24	182.206.127.117	China	1
25	70.182.144.165	United States	91
26	174.29.187.213	United States	60
27	74.136.78.137	United States	41
28	76.221.152.218	United States	1
29	97.83.20.210	United States	61
30	67.243.183.241	United States	13
31	66.210.54.210	United States	105

There are Unique IP address column, country and hit column.

3. Activity



Script makes activity directory. And make (unique IP address).csv per unique IP address.

	A	B	C	D	E	F	G	H	I	
1	2015-11-29	20:05:54	172.17.100.5	GET	/nut/landing/1/43a67e8d-c0e0-4fd6-b125-28e1acaa3098	-	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
2	2015-11-29	20:05:56	172.17.100.5	GET	/Nut/Home/CampaignExpired	-	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
3	2015-11-29	20:05:56	172.17.100.5	GET	/Nut/Content/css/cssbundle	v=Y93NHXh-TyywGmNI5YrmLIyMFUTqaUXtHTtoq4p850E1	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
4	2015-11-29	20:05:57	172.17.100.5	GET	/Nut/Content/themes/base/cssbundle	v=4U2IrngsdNvnRYqp1SXQZr_N9G8HjH_JFK0uqkGm9kE1	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
5	2015-11-29	20:05:58	172.17.100.5	GET	/Nut/Scripts/modernizrbundle	v=RXYNTxBZ6eQfZC6W5SJcrhKrCXLWPkmJo_evtyEK7_g1	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
6	2015-11-29	20:06:00	172.17.100.5	GET	/Nut/Scripts/customjsbundle	v=CfveTlz0dhBmc3wbPb00EpKxou_ZhLhQ5xsGamTXzKA1	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)
7	2015-11-29	20:06:10	172.17.100.5	GET	/Nut/Scripts/jquerybundle	v=X-V-OevTiZHD2uYLseBQznCuJ_FGsW3qdfE87fEckGQ1	443	-	2.36.98.96	Mozilla/5.0 (Windows NT 6.1; WOW64)

Each csv file has all fields of log format as column.

4. sqli_list.csv

	A	B	C	D	E	F
1	2015-12-21	01:03:32	172.17.100.8	GET	/corporate_info.php	content=corp_mgt" and "x"="x
2	2015-12-21	01:03:32	172.17.100.8	GET	/corporate_info.php	content=corp_mgt" and "x"="y
3	2015-12-21	01:03:36	172.17.100.8	GET	/corporate_info.php	content=corp_mgt" or (1,2)=(select*from(select name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,108,111,108,111,115,104,101,114),1))a) -- "x"="x
4	2015-11-29	07:46:02	172.17.100.5	GET	/Error/NotFound	'
5	2015-11-29	07:46:33	172.17.100.5	GET	/Content/css/cssbundle	'
6	2015-11-29	07:46:34	172.17.100.5	GET	/Content/themes/base/cssbundle	'

As above, this csv file has all fields of log format as column too.

R
Detects classic SQL injection probings 1/2
Detects classic SQL injection probings 1/2
Detects classic SQL injection probings 1/2
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters
Regex for detection of SQL meta-characters

At last column is reason why this line is detected as SQL injection.

5. rfi_list.csv

68	2015-11-26	17:43:47	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//download
69	2015-11-26	17:43:50	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//download
70	2015-11-26	17:43:51	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//download
71	2015-11-26	17:43:53	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//download
72	2015-11-26	17:43:55	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//download
73	2015-11-26	17:43:59	172.17.100.8	GET	/bdgdb/file_manager.php	goto=C:/Repository/Web/REDACTED.com//templates
74	2015-11-26	18:53:31	172.17.100.8	GET	/ext_affiliate.php	content=aff_about'A=0
75	2015-11-26	18:54:26	172.17.100.8	GET	/bdgdb/modules.php	set=payment&selected_box=modules
76	2015-11-26	18:54:28	172.17.100.8	GET	/bdgdb/modules.php	set=payment&selected_box=modules
77	2015-11-26	18:54:29	172.17.100.8	GET	/bdgdb/modules.php	set=payment
78	2015-11-29	07:44:47	172.17.100.5	GET	/Error/NotFound	<script>alert('TK00000005')</script>
79	2015-11-29	07:44:48	172.17.100.5	GET	/Error/NotFound	<script>alert('TK00000006')</script>

This csv's columns are same ass sqli_list.csv. There are detected line as remote file inclusion.

6. webshell_list.csv

303	2015-11-29	07:37:48	172.17.100.5	GET	/_cti_pvt/LICENSE.php	-	80
304	2015-11-29	07:43:50	172.17.100.5	GET	/abo.php	-	443
305	2015-11-29	07:43:50	172.17.100.5	GET	/c99.php	-	443
306	2015-11-29	07:43:50	172.17.100.5	GET	/c100.php	-	443
307	2015-11-29	07:43:50	172.17.100.5	GET	/default.php	-	443
308	2015-11-29	07:43:52	172.17.100.5	GET	/k4m1kz.php	-	443
309	2015-11-29	07:43:52	172.17.100.5	GET	/loginz.php	-	443
310	2015-11-29	07:43:52	172.17.100.5	GET	/macedonia.php	-	443
311	2015-11-29	07:43:52	172.17.100.5	GET	/r57.php	-	443
312	2015-11-29	07:43:53	172.17.100.5	GET	/reply.php	-	443
313	2015-11-29	07:43:53	172.17.100.5	GET	/shell.php	-	443
314	2015-11-29	07:43:54	172.17.100.5	GET	/sniper.php	-	443
315	2015-11-29	07:43:54	172.17.100.5	GET	/LICENSE.php	-	443
316	2015-11-29	07:43:55	172.17.100.5	GET	/Error/abo.php	-	443
317	2015-11-29	07:43:55	172.17.100.5	GET	/Error/c99.php	-	443
318	2015-11-29	07:43:55	172.17.100.5	GET	/Error/c100.php	-	443
319	2015-11-29	07:43:55	172.17.100.5	GET	/Error/default.php	-	443
320	2015-11-29	07:43:55	172.17.100.5	GET	/Error/k4m1kz.php	-	443
321	2015-11-29	07:43:55	172.17.100.5	GET	/Error/loginz.php	-	443

This csv's columns are same sqi_list.csv and rfi_list.csv. this lines are detected because of famous web shell name.