

CLUB ETHICAL HACKING

Edition 2019/2020



Séance #3
OneSmile Inc.
Part.2 Forensic

8 Janvier 2020



Point de contact

Rémi ALLAIN <rallain@cyberprotect.one>

Daniel DIAZ <ddiaz@cyberprotect.one>

CORRECTION / Rappel des objectifs

Sur **Kibana**, choisissez la période allant de **2019-11-27 6am** à **2019-11-27 2pm**

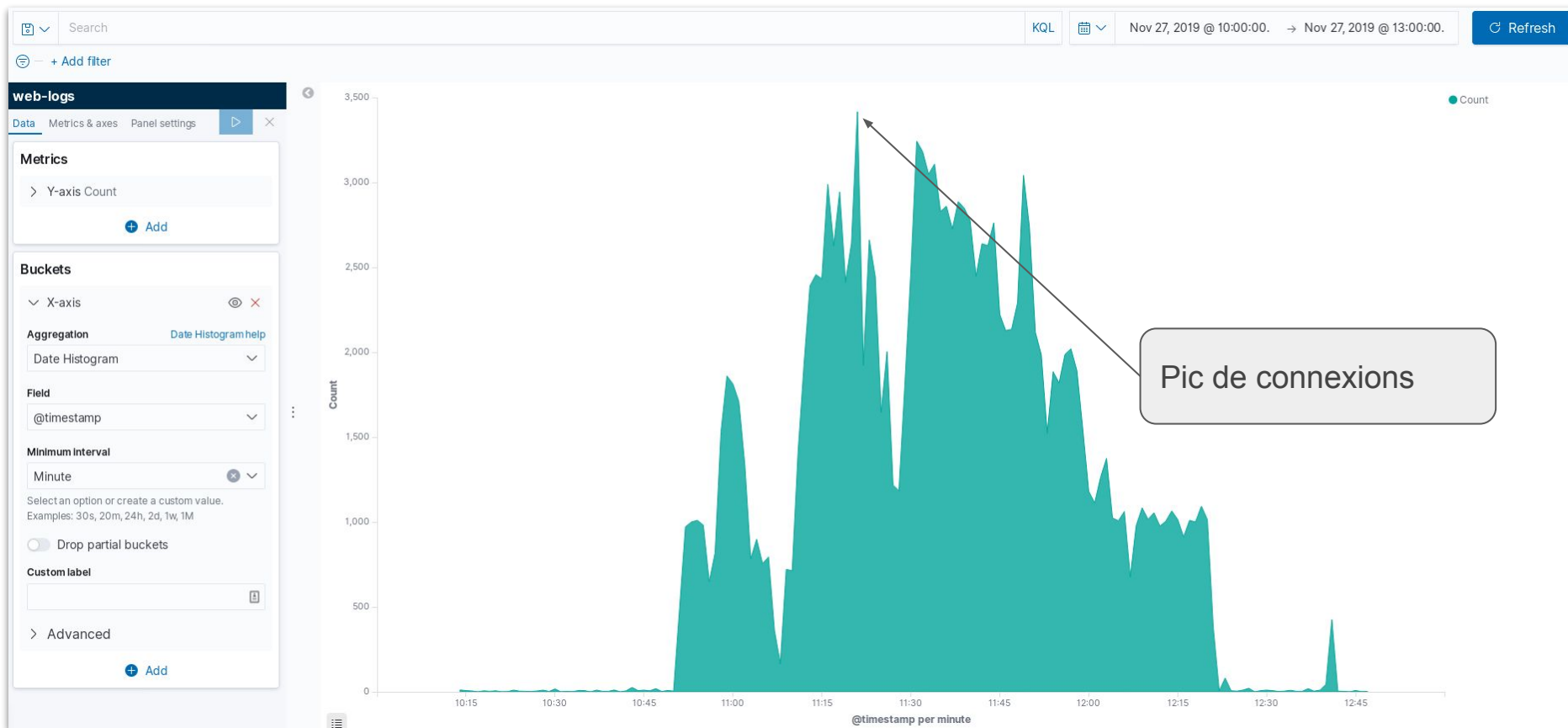
Les deux indices à analyser sont **web-logs** et **web-logs-full**

1. À quelle période, un pic de connexion a-t-il été enregistré ? (à 5 minutes près)
2. Combien de personnes distinctes se sont connectées au serveur ?
 - Comment les avez-vous identifiées ?
3. Quel est le top 10 des comportements suspects ? (les attaques / scans qui reviennent le plus souvent)
4. Quelle est l'attaque qui a été la plus visible ? (la moins discrète)
5. Identifier les tentatives de brute-forcing
6. Identifier les processus de crawling

Documentation de Kibana: <https://www.elastic.co/guide/en/kibana/current/index.html>

(Les parties qui nous intéressent sont Discover et Analyze)

CORRECTION / Question 1



CORRECTION / Question 2

Search [KQL] Nov 27, 2019 @ 10:00:00. → Nov 27, 2019 @ 13:00:00. Refresh

web-logs

Data Options

Metrics

> Metric Count

+ Add

Buckets

Split rows

Aggregation Terms

Field transaction.remote_address.keyword

Order by Metric: Count

Order Descending Size 1000

Group other values in separate

Remote address	Count	Count percentages
37.165.144.158	86,789	54.6%
81.185.162.78	64,167	40.4%
92.184.101.8	6,984	4.4%
196.52.10.11	263	0.2%
194.99.104.28	124	0.1%
185.210.219.156	105	0.1%
185.212.170.188	103	0.1%
23.92.127.34	101	0.1%
80.215.115.179	85	0.1%
185.220.70.152	61	0%
103.208.220.130	39	0%
83.31.132.5	8	0%
109.74.197.184	6	0%
37.166.26.234	6	0%
95.25.79.209	6	0%
158,898		

Export: Raw Formatted

En agrégeant sur le champ remote_address, on obtient la liste unique des IP qui se sont connectées.

Cette variable à elle seule ne permet pas d'identifier un utilisateur.

CORRECTION / Question 2

Search

KQL

Nov 27, 2019 @ 10:00:00. → Nov 27, 2019 @ 13:00:00.

Refresh

+ Add filter

web-logs



Data Options


Metrics

Metric Count

Add

Buckets

Split rows transaction.remot...  

Split rows request.headers....  

Add

Remote address	request.headers.User-Agent.keyword: Descending	Count	Count percentages
37.165.144.158	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	16,941	11.8%
37.165.144.158	track-fantastic/vortex-2.4	13,217	9.2%
37.165.144.158	() { : ; },echo 93e4f0-CVE-2014-6271: true;echo;echo;	9,053	6.3%
81.185.162.78	() { : ; },echo 93e4f0-CVE-2014-6271: true;echo;echo;	5,814	4%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	4,192	2.9%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	2,345	1.6%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,925	1.3%
37.165.144.158	() { : ; },echo Nikto-Added-CVE-2014-6271: true;echo;echo;	1,938	1.3%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	1,675	1.2%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	1,761	1.2%
92.184.101.8	() { : ; },echo 93e4f0-CVE-2014-6271: true;echo;echo;	1,513	1.1%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,419	1%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	669	0.5%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	456	0.3%
37.165.144.158	Mozilla/5.0 (Windows NT 5.1; U; de) Opera 8.50	449	0.3%
		143,985	

Export: Raw Formatted

En ajoutant à notre précédent agrégat le champ User-Agent, on affine l'identification des utilisateurs.

Même si, ce n'est toujours pas pertinent. On remarque dans les User-Agent des mots clés comme "Nikto", un outil de scan web.

CORRECTION / Question 2

Search

KQL

Nov 27, 2019 @ 10:00:00. → Nov 27, 2019 @ 13:00:00.

Refresh

+ Add filter

web-logs

Data

Options

Metrics

Metric Count

+ Add

Buckets

Split rows transaction.remot... @ = ×

Split rows request.headers.... @ = ×

Split rows request.headers.... @ = ×

+ Add

Remote address

request.headers.User-Agent.keyword: Descending

request.headers.Cookie.keyword: Descending

Count

Count percentages

81.185.162.78	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	PHPSESSID=63af36e7879efa891fdd7c061c34a2c0	190	12.1%
37.165.144.158	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	PHPSESSID=5aec1112f3fda56f8afb989960a2b5	133	8.5%
196.52.10.11	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	PHPSESSID=c98881052e99b7c8d82b3d22527b8118	109	7%
23.92.127.34	Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25	PHPSESSID=f7e7c38703491d99744c5fc03424878c	98	6.3%
185.212.170.188	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	PHPSESSID=8aaaa36b1e8d23250999aa23d46873f9	98	6.3%
194.99.104.28	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0	PHPSESSID=fd043b951176e9ec5fa15e74b14ff99e	98	6.3%
196.52.10.11	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0	PHPSESSID=292dc9075e1b853690d7f2cbbfb942d4	92	5.9%
185.210.219.156	Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25	PHPSESSID=15d4e3448560929a102282c1b255d618	90	5.7%
37.165.144.158	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	PHPSESSID=8c491a0371fbcc4d7f6a8df2e04f3b0a	86	5.5%
37.165.144.158	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	PHPSESSID=4aad98fefeca0132e613fb48718de12	65	4.1%
196.52.10.11	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	PHPSESSID=26cd08e9dd4441289b93b98728b8359f	47	3%
37.165.144.158	track-fantastic/vortex-2.4	PHPSESSID=b4d171a2a1c2aa3b1406aca069909466	41	2.6%
37.165.144.158	Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0	PHPSESSID=d6c1a0822ed6318f465eca1ba645e9ee	40	2.6%
185.220.70.152	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0	PHPSESSID=ac5601aed7d39d2a439d7519c115b2d	37	2.4%
103.208.220.130	Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25	PHPSESSID=35569b73e5b376041a284838	28	1.8%

Export: Raw Formatted

En ajoutant à notre précédent agrégat le champ Cookie, et notamment sa valeur PHPSESSID, on arrive à identifier plus clairement les utilisateurs.

C'est le mieux que nous puissions faire avec ces données. Même si des données sont omises ou caduques.

CORRECTION / Question 3

Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. : Audit message

IP	User-Agent	Count	Count percentages
37.165.144.158	() { ;; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	9,053	16.3%
81.185.162.78	() { ;; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	5,814	10.5%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	4,192	7.5%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	2,345	4.2%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,919	3.5%
37.165.144.158	() { ;; }; echo Nikto-Added-CVE-2014-6271: true;echo;echo;	1,938	3.5%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	1,761	3.2%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	1,675	3%
92.184.101.8	() { ;; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	1,513	2.7%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,413	2.5%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	669	1.2%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)		
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)		
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)		
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)		

En effectuant une agrégation par table et par ligne, on obtient un tableau d'attaquant pour chaque type de détection.

Ici il s'agit d'un refus d'accès au serveur; Ce refus est déclenché lorsque le module de sécurité d'apache, détecte des comportements anormaux: Brute force, Injections, etc.

CORRECTION / Question 3

Warning. Operator GE matched 5 at TX:inbound_anomaly_score. : Audit message

IP	User-Agent	Count	Count percentages
37.165.144.158	() { :; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	9,053	16.3%
81.185.162.78	() { :; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	5,814	10.5%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	4,192	7.5%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	2,345	4.2%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,919	3.5%
37.165.144.158	() { :; }; echo Nikto-Added-CVE-2014-6271: true;echo;echo;	1,938	3.5%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	1,761	3.2%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	1,675	3%
92.184.101.8	() { :; }; echo 93e4r0-CVE-2014-6271: true;echo;echo;	1,513	2.7%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,413	2.5%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	669	1.2%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	454	0.8%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi_dir_check)	203	0.4%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		

On remarque que ces scores d'anomalies sont principalement déclenchés par NIKTO

CORRECTION / Question 3 et 4

Warning. Matched phrase "nikto" at REQUEST_HEADERS:User-Agent : Audit message

IP	User-Agent	Count	Count percentages
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	4,192	10.7%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	2,345	6%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,919	4.9%
37.165.144.158	() { :: }; echo Nikto-Added-CVE-2014-6271: true;echo;echo;	1,938	4.9%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000964)	1,761	4.5%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	1,675	4.3%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	1,413	3.6%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitefiles)	669	1.7%
92.184.101.8	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)	454	1.2%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000108)	225	0.6%
37.165.144.158	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi_dir_check)	203	0.5%
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		
81.185.162.78	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)		

Cette règle confirme nos précédents dire.

On peut dès lors établir, qu'il s'agit de "l'attaque" la plus visible.

CORRECTION / Question 5

Search

KQL

Nov 27, 2019 @ 10:00:00. → Nov 27, 2019 @ 13:00:00.

Refresh

web-logs-full

Data

Options

Metrics

> Metric Count

Add

Buckets

> Split rows requestBody.keyword...

Add

requestBody.keyword: Descending	Count	Count percentages
MYDATA	30,210	38.6%
<!--#include virtual="/index.jsp"-->	28,463	36.4%
method=open+service%3a3%2e0%2e2%2e1105&service%5fname=%2f	6,760	8.6%
num_lines=1000&log_location=..%2F..%2F..%2F..%2Fetc%2Fpasswd	6,247	8%
dump_sql=foo	2,874	3.7%
;	1,154	1.5%
dir=/ my_post_key=&keywords='+or+'a'+a&quick_search=Search+PMs&allbox=Check+All&fromfid=0&fid=4&jumpto=4&action=do_stuff	952	1.2%
<script>alert('XSS')</script>[]=PATH DISCLOSURE	530	0.7%
object=1;system('id');	438	0.6%
transaction_id=1&oauth_token="%3becho"	204	0.3%
button.login.home=Se%20connecter&Login.userAgent=0x4148_Fu&reload=0&SSLPVNUser.Password=0x4148Fu&SSLPVNUser.UserName=0x4148&thispage=../../../../etc/passwd%00	122	0.2%
button.login.home=Se%20connecter&Login.userAgent=0x4148_Fu&reload=0&SSLPVNUser.Password=0x4148Fu&SSLPVNUser.UserName=0x4148&thispage=../../../../etc/passwd%00	98	0.1%
userName=admin&password=axis2&submit+=Login+	32	0%
0=1234	24	0%
username=admin&password=admin		

Export: Raw Formatted

En analysant le corps des requêtes on peut identifier les processus de brute-forcing et de scan.

Notamment au niveau du formulaire d'authentification, sur lequel on peut également voir des tentatives d'injections.

Des questions ? → **rallain@cyberprotect.one**