The Honeynet PROJECT

L’analyse de logs

Sébastien Tricaud
Groupe Resist - Toulouse 2013

whoiam

- Principal Security Strategist @Splunk
- Co-Fondateur de la société Picviz Labs
- Ancien CTO du projet Honeynet
- Co-lead du chapitre Honeynet français
- Contributeur de nombreux logiciels open-source : Prelude IDS, OSSEC, Linux PAM, faup, etc.

Qu’est-ce qu’un log ?

- Un fichier texte ou binaire
- Du traffic réseau
- Une base de données
- …

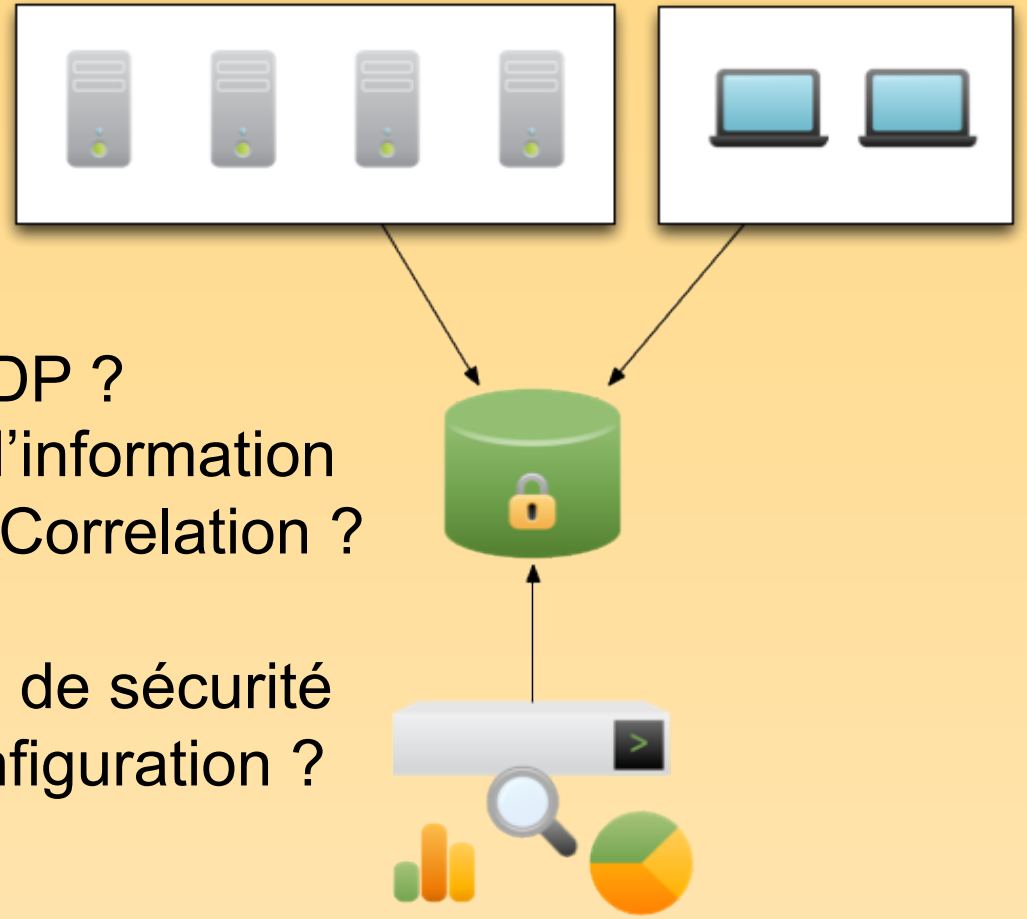
Exemple de taille de logs

Capture par netflow d'un pays de 45 millions d'habitants sur le backbone principal

=

3 millions d'évènements / 5 min

Log Management



- Syslog UDP ?
- Partage d'information
- Alertes ? Correlation ?
- Volume ?
- Problème de sécurité ou de configuration ?

À la recherche du TLD perdu

Nous souhaitons extraire tous les domaines en “.ru” d’un fichier de proxy

```
$ grep "\.ru" squid.log
```

À la recherche du TLD perdu

[...] "[28/Feb/2011:00:13:02 +0100]" XXXX GET http://pixel.quantserve.com/pixel;r=1869975797;fpan=0;fpa=P0-1991180462-1298650127845;ns=1;url=http%3A%2F%2Foptimized- by.rubiconproject.com%2Fa%2F3346%2F3 [...]

[...] "[28/Feb/2011:00:14:32 +0100]" xgbj352 GET http://eco.rue89.com/2011/02/25/oui-les-militaires-meritent- leur-reduction-de-75-a-la-sncf-192164?page=0 HTTP/1.1 500 1120 500 505 TCP_NC_MISS 567 12 1103 10.33.37. [...]

À la recherche du TLD perdu

grep -e avec la bonne regex

'http(s)?\://[a-zA-Z0-9\-\:\.]+\.(ru)/'

À la recherche du TLD perdu

[...] "[28/Feb/2011:02:02:08 +0100]" XXXX GET http://www.facebook.com/plugins/like.php?href=http:/ /slon.**ru**/articles/XXXX [...]

La regex la plus compliquée du monde!

^(http|https|ftp)\://([a-zA-Z0-9\.\-]+(\:[a-zA-Z0-9\.&%\$\-]+)*@)?
((25[0-5]|2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9])\.(25[0-5]|
2[0-4][0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]|0)\.(25[0-5]|2[0-4]
[0-9]|[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[1-9]|0)\.(25[0-5]|2[0-4][0-9]|
[0-1]{1}[0-9]{2}|[1-9]{1}[0-9]{1}|[0-9])|([a-zA-Z0-9\-]+\.)*[a-zA-Z0-9\-]
+\.[a-zA-Z]{2,4})(\:[0-9]+)?(/[^/][a-zA-Z0-9\.\,\?\'\\/\+&%\$#\=~_
\-@]*)*$

Faites votre marché

http://www.regexlib.com/Search.aspx?k=url

Problème liés à grep

- Encodage des caractères
- Obtenir les lignes de logs manquées

Faup: Finally an URL parser

http://www.github.com/stricaud/faup

- Extracteur de champs d'url universel, rapide (0 allocation) et résistant aux urls moisies
- Bibliothèque en C, bindings Python, outil en ligne de commande

```
$ faup -p https://www.ossir.org/index.php?a=http://slashdot.org
scheme,credential,subdomain,domain,host,tld,port,resource_path,query_string,fragment
https,,www,ossir.org,www.ossir.org,org,,/index.php,?a=http://slashdot.org,
```

Faup: Finally an URL parser

```
$ faup https://www.ossir.org/index.php?a=http://slashdot.org |cut -d, -f6
org

$ faup https://www.ossir.org/index.php?a=http://slashdot.org |cut -d, -f9 |cut -d= -f2
http://slashdot.org

$ faup https://www.ossir.org/index.php?a=http://slashdot.org |cut -d, -f9 |cut -d= -f2 |faup
http,,,,slashdot.org,org,,,,
```

Comment récupérer les informations pertinentes ?

- Normaliser puis faire correspondre avec des signatures pour extraire des alertes de sécurité

- Faire n'importe quoi!

Signature OSSEC

```
<rule id="5715" level="3">
  <if_sid>5700</if_sid>
  <match>^Accepted|authenticated.$</match>
  <description>SSHD authentication success.</description>
  <group>authentication_success,</group>
 </rule>

<rule id="5716" level="5">
  <if_sid>5700</if_sid>
  <match>^Failed|^error: PAM: Authentication</match>
  <description>SSHD authentication failed.</description>
  <group>authentication_failed,</group>
 </rule>
```

Démo : faire n'importe quoi!

- Nous allons par exemple chercher des logs intéressants par longueur de texte

Know Your Enemy

Les logs configurables !

Squid

Configuration du format de log

logformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt

Options

- [http::]rm Request method (GET/POST etc)
- [http::]ru Request URL
- [http::]rp Request URL−Path excluding hostname
- ...

ProFTPd

- Les logs sont gérés par mod_log

Configuration du format de log

LogFormat default "%h %l %u %t \"%r \" %s %b "

Options

%A − Utilisateur anonyme (mot de passe donné)

%a − Adresse IP du client

%b − Octets envoyés pour le requête

ProFTPd

- L'option %A est fort intéressante!

- Code gérant cette option :

```
#define PR_TUNABLE_PATH_MAX 1024
char arg [PR_TUNABLE_PATH_MAX+1] = { ' \ 0 ' } ;
        case META_ANON_PASS:
                argp = arg ;
                pass = pr_table_get(session.notes,
"mod_auth.anon−passwd", NULL);
                if (!pass) pass = "UNKNOWN";
                sstrncpy(argp, pass, sizeof(arg));
```

ProFTPd

- Injection possible dans /var/log/proftpd/ auth.log

Conclusion

- Il ne faut pas chercher des authentifications ssh dans le log de proftpd
- Il n'y a pas de base de données centralisant ces problèmes

Base de données liées aux problèmes de log

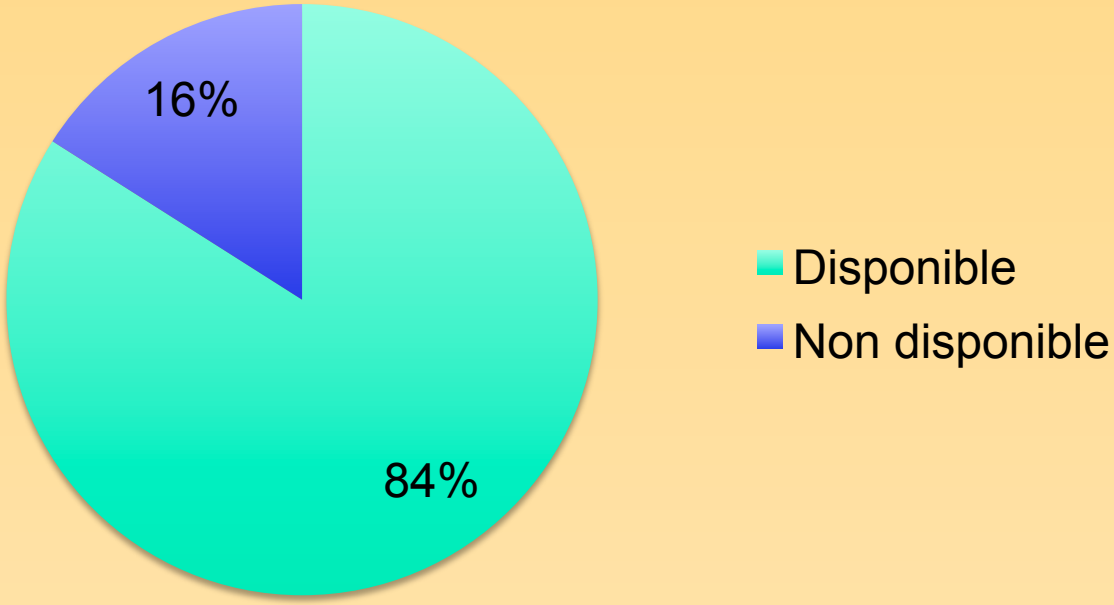
- Il existe CWE “Common Weakness Enumeration”

- CWE-778: Insufficient Logging
  "*When a security-critical event occurs, the software either does not record the event or omits important details about the event when logging it.*"

Quelques “failles de logs” dans CVE

- CVE-2003-1566: Microsoft IIS 5.0 does not log requests that use the TRACK method, which allows remote attackers to obtain sensitive information without detection.
- CVE-2007-3730: OpenVMS does not log the source IP.
- CVE-2008-1203: Adobe ColdFusion 8 and ColdFusion MX7 do not log failed connection attempts on the administrative interface.
- ...

Disponibilité d'évidence d'intrusion dans les logs



Source : Verizon 2012 "Data Breach Investigation Report"

Question ?

@tricaud

sebastien@honeynet.org
stricaud@splunk.com