Détection d'intrusions
Travaux pratiques

Bureaux Supervision de Sécurité Globale
ANSSI/SDO/DD

Programme

- Introduction aux analyses de détection d'intrusion réseau
- Méthode d'analyse
  - Qualifications d'évènements
  - Prises de décisions
- Introduction à la conception de signatures IDS
- Exercices
  - Détection de compromission d'un serveur WEB
  - Détection de compromission d'un poste de travail

MÉTHODOLOGIE

Qualification d'évènements

- Qui ?
  - Qui communique avec qui ?
- Comment ?
  - Quels sont les protocoles utilisés ?
- Combien ?
  - Quelle quantité de données a été échangée ?
- Quand ?
  - Quand le comportement a-t-il débuté ? Qu'elles étaient les horaires ?

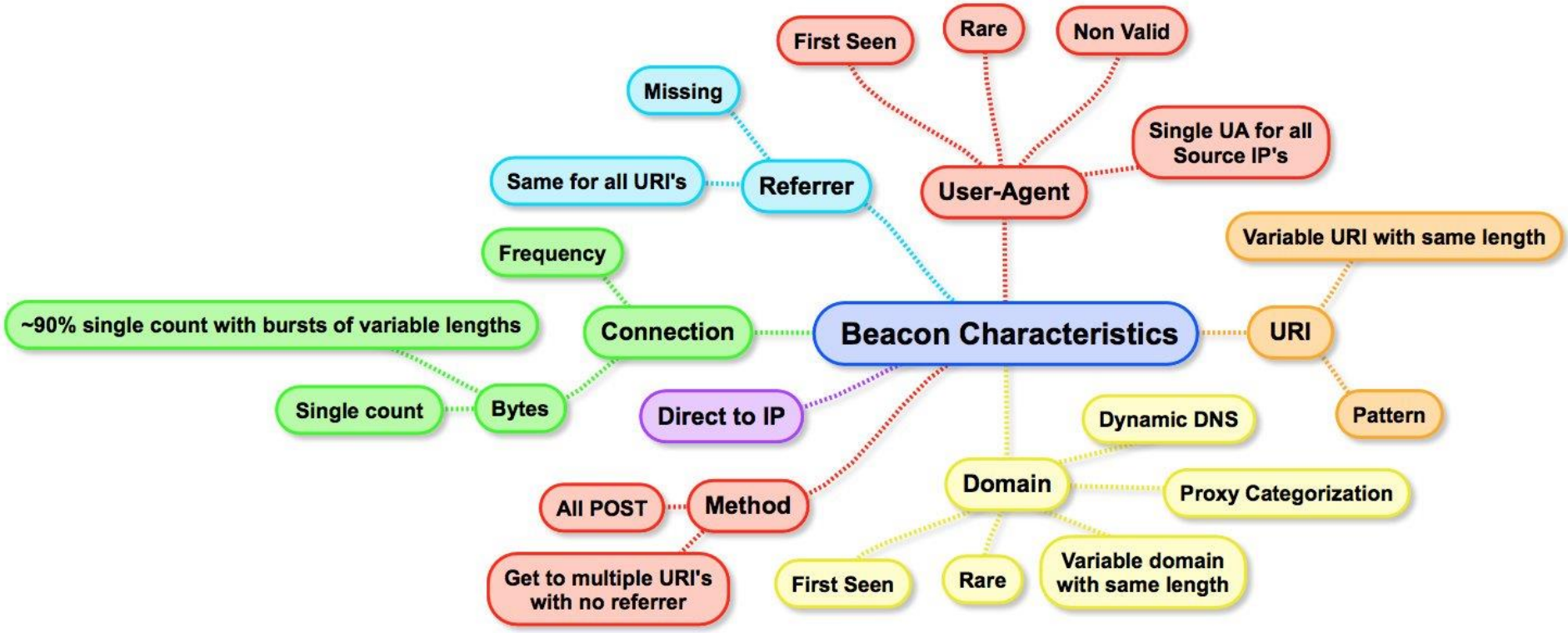
Recherche d'activité suspecte

- Port et service non commun
- Flux
  - Fréquence
  - Récurrence
  - Taille de paquets
  - Catégoriser les types de flux
  - Liste blanche sur les flux légitimes
  - Grande quantité de données en Upload
- Services d'administration à distance
- Rechercher des motifs connus d'attaques
  - Header HTTP, User-agent non commun, SQLi, etc

Recherche d'activité suspecte

- Activité sur plage horaire non fréquente
- Type de fichier exécutable
  - Non lié à des mises à jour ou installations légitimes

Recherche d'activité suspecte



Recherche d'activité suspecte

Attention portée sur les points suivants

- Traffic chiffré
- Proxy / VPN / TOR
- Origine de l'attaque
  - Serveur contrôlé
  - Serveur mutualisé
  - Serveur compromis

Finalité d'une analyse de détection

Qualification d'évènements et prise de décision

- Tentative d'intrusion
  - Capitalisation
- Vrai positif - Compromission
  - Transmission des éléments pour une réponse à incident
- Faux positif
  - Requalification de signature
  - Amélioration continue
- Levée de doute
  - Eléments complémentaires nécessaires à la prise de décision

Objectifs

- Comprendre les formats de logs et appliquer des traitements
- Simplifier l'analyse d'un grand nombre de données
- Identifier les comportements légitimes/illégitimes
- Synthétiser et qualifier les évènements

Contexte

- Serveur Web exposé sur internet

- 3 applications hébergées sur le site anssi.fr
  - Wiki (lecture et modification de pages)
  - Wordpress (galerie photo)
  - Team_info (lecture d'information de membres depuis base de données)

Apache

- Serveur Apache :
  - Logs : /var/log/apach2/access.log
  - Chaque requête est journalisée
  - Logs bruts

```
IP_Source - - [ Date ] "Requête (methode uri version)" Code_retour Taille_réponse
"Referer" "User-Agent"
```

```
213.245.154.160 - - [06/Mar/2020:16:46:31 +0100] "GET /dokuwiki/doku.php?id=linux:admin
HTTP/1.1" 200 8779 "http://anssi.fr/dokuwiki/doku.php?id=linux:admin&do=edit"
"Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0"
```

Comprendre un événement

```
213.245.154.160 - - [06/Mar/2020:16:46:31 +0100] "GET /dokuwiki/doku.php?id=linux:admin
HTTP/1.1" 200 8779 "http://anssi.fr/dokuwiki/doku.php?id=linux:admin&do=edit" "Mozilla/5.0
(X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0"
```

- Que fait le client
  - Qui (adresse source, user agent, date)
    - *213.245.154.160,*
    - *Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0*
  - Quoi (URI)
    - */dokuwiki/doku.php?id=linux:admin*
  - Comment (méthode, referer)
    - *GET*
    - *http://anssi.fr/dokuwiki/doku.php?id=linux:admin&do=edit*
- Qu'obtient t il ? (Code retour, taille réponse)
  - *200 → code succès*
  - *8779 bytes*

Classification des événements

> Comportements observables sur un serveur web

Requêtes	Humaines	Non-humaines
Légitimes	Navigations d'administrateurs Navigations de clients	Robots d'indexation
Illégitimes	Tentatives d'accès à des ressources non indexées (énumération, LFI…) Injections de paramètres forgés (SQLi, XSS…)	Scanneurs de vulnérabilités

Traitement des événements

- 2 moyens d'analyser des journaux
  - Outils d'indexation et de visualisation (Splunk, stack ELK…)
  - Commandes built-in GNU/Linux (gawk, grep, less…)

- Commandes utiles sous GNU/Linux
  - Gawk –F « » '{if ($i == 200) print $j}' path/to/file
    - *Affiche les valeurs de la colonne j lorsque la colonne i vaut 200*
    - *i et j correspondent aux numéros de colonnes ($1 : col 1, $2 : col 2, $0 : toutes les col)*
  - Grep « toto » path/to/file
    - *Affiche toutes les lignes du fichier comportant le motif toto*
  - Less –S path/to/file
    - *Affiche le contenu d'un fichier dans une fenêtre dynamique*
  - Sort (-n) : Trie en fonction du premier caractère (du premier nombre)
  - Uniq (-c) : Affiche les valeurs uniques (et les compte)

Contexte

- Serveur Apache connecté à internet
- 3 applications hébergées sur le site (anssi.fr)
  - Wiki (lecture et modification de pages)
  - Wordpress (gallerie photo)
  - 'Team_info' (lecture d'information de membres depuis base de données)
- Fichier de log : ~ 8000 entrées
- Informations de contexte → gain de temps considérable lors de l'analyse