

Travaux pratiques – Isoler un hôte compromis en utilisant un 5-tuple

Objectifs

Au cours de ces travaux pratiques, vous allez passer en revue les journaux documentant une faille afin de déterminer les hôtes et le fichier compromis.

Partie 1: Consulter les alertes dans Sguil.

Partie 2: Passer à Wireshark.

Partie 3: Passer à Kibana

Contexte/scénario

Le quintuplé est utilisé par les administrateurs IT afin d'identifier les conditions requises pour créer un environnement de réseau opérationnel et sécurisé. Les composants de ce quintuplé incluent une adresse IP et un numéro de port sources, une adresse IP et un numéro de port cibles, ainsi que le protocole utilisé dans la charge utile de données. Il s'agit du champ de protocole de l'en-tête de paquet IP.

Au cours de ces travaux pratiques, vous allez également consulter les journaux pour identifier les hôtes compromis et le contenu du fichier infecté.

Ressources requises

- La machine virtuelle Security Onion

Instructions

Après l'attaque, les utilisateurs n'ont plus accès au fichier **confidential.txt**. Vous allez maintenant passer en revue les journaux pour déterminer comment le fichier a été compromis.

Remarque: lorsqu'il s'agit d'un réseau de production, nous recommandons aux utilisateurs **analyst** et **root** de modifier leur mot de passe et de respecter la politique de sécurité en vigueur.

Partie 1: Consultez les alertes dans Sguil.

- Ouvrez une session sur la machine virtuelle Security Onion avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.
- Ouvrez **Sguil** et connectez-vous. Cliquez sur **Select All**, puis sur **Start SGUIL**.

- c. Passez en revue les événements répertoriés dans la colonne Event Message. Un de ces messages est **GPL ATTACK_RESPONSE id check returned root**. Ce message indique qu'un hacker a pu obtenir un accès root. L'hôte à l'adresse 209.165.200.235 a renvoyé un accès root à 209.165.201.17. L'ID d'alerte **5.1** est utilisé dans ce TP.

RealTime Events												Escalated Events											
ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP	DPort	Pr	Event Message												
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root												
RT	351	seconion-ossec	1.1	2020-06-19 18:09:28		0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.												
RT	23	seconion-ossec	1.2	2020-06-19 18:09:29		0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.												

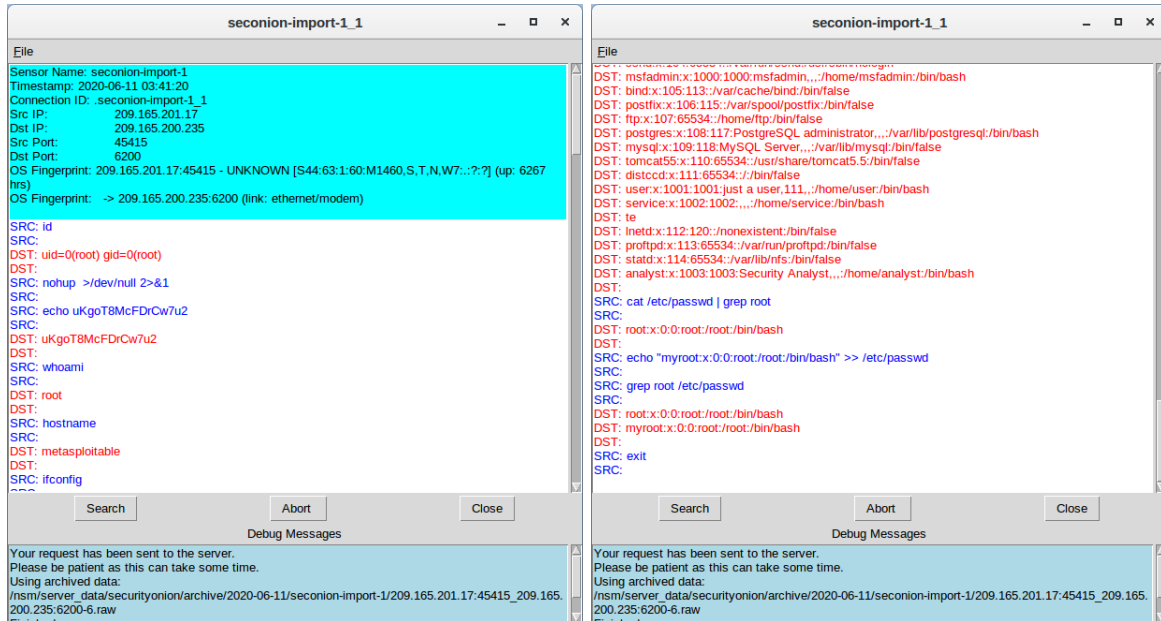
- d. Cochez les cases **Show Packet Data** et **Show Rule** pour afficher chaque alerte plus en détail.



- e. Cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.1 et sélectionnez **Transcript**.

RealTime Events Escalated Events									
ST	CNT	Sensor	Alert ID	Date/Time	Δ	Src IP	SPort	Dst IP	DPort
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20		209.165.200.235	6200	209.165.201.17	
RT	351	seconion-ossec	Event History	09:28		0.0.0.0		0.0.0.0	
RT	23	seconion-ossec	Transcript	09:29		0.0.0.0		0.0.0.0	
RT	7	seconion-ossec	Transcript (force new)	10:04		0.0.0.0		0.0.0.0	
RT	7	seconion-ossec	Wireshark	10:04		0.0.0.0		0.0.0.0	

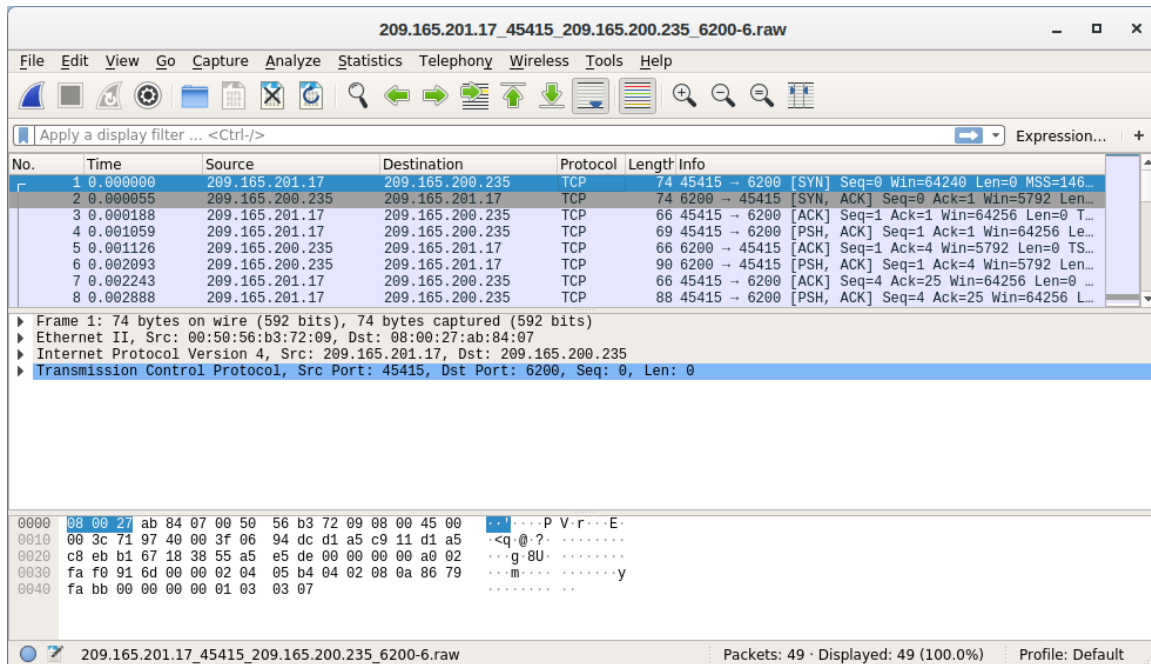
- f. Examinez les transcriptions de toutes les alertes. La transcription affiche les transactions entre la source de l'acteur de menace (SRC) et la cible (DST) pendant l'attaque. L'acteur de menace exécute des commandes Linux sur la cible.



Quel type de transactions s'est produit entre le client et le serveur dans cette attaque?

Partie 2: Passez à Wireshark.

- Sélectionnez l'alerte qui vous a fourni la transcription de l'étape précédente. Cliquez avec le bouton droit sur l'ID d'alerte 5.1, puis sélectionnez **Wireshark**. La fenêtre principale de Wireshark affiche 3 vues d'un paquet.



- Pour afficher tous les paquets qui sont assemblés dans une conversation TCP, cliquez avec le bouton droit sur n'importe quel paquet, puis sélectionnez **Follow > TCP Stream**.



Qu'avez-vous observé ? Qu'indiquent les couleurs de texte rouge et bleu ?

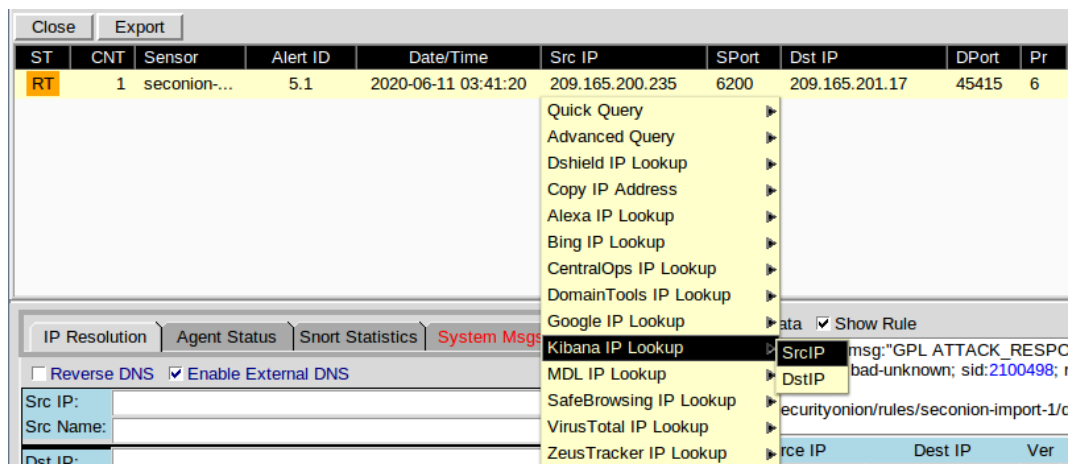
L'attaquant exécute la commande **who am i** sur la cible. Qu'est-ce que cela montre sur le rôle de l'attaquant sur l'ordinateur cible ?

Faites défiler le flux TCP. Quel type de données l'acteur de la menace a-t-il lu ?

- c. Quittez la fenêtre du flux TCP. Lorsque vous avez terminé d'examiner les informations fournies par **Wireshark**, fermez-le.

Partie 3: Passez à Kibana

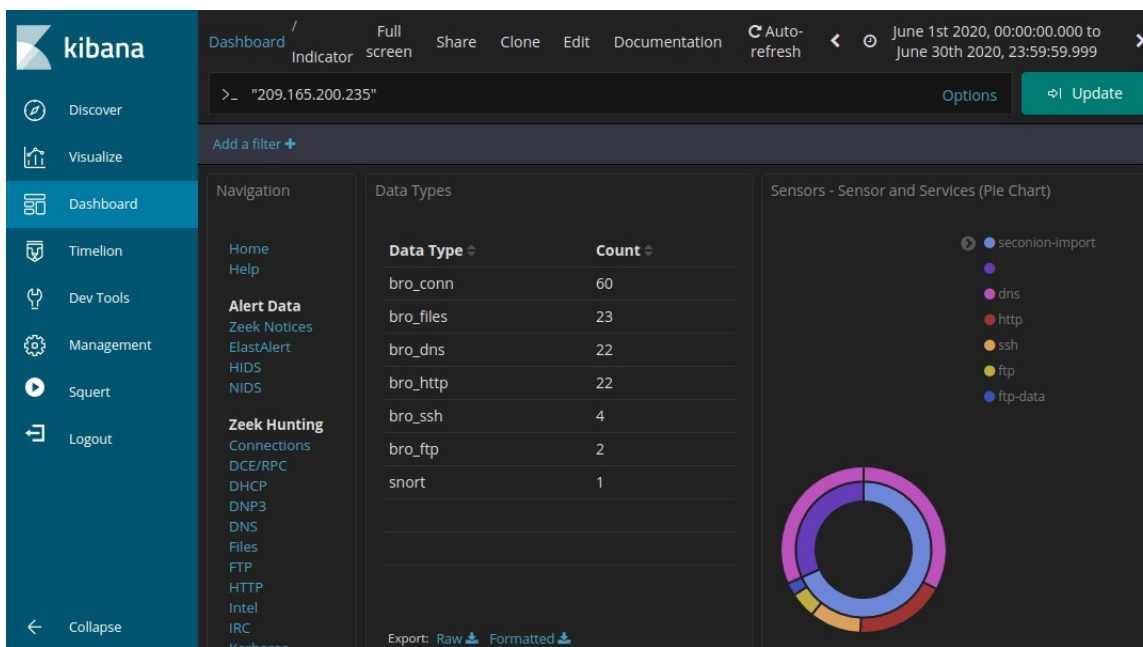
- a. Retournez dans Sguil. Cliquez avec le bouton droit sur l'adresse IP source ou de destination pour l'ID d'alerte 5.1 et sélectionnez **Kibana IP Lookup > SRCip**. Saisissez le nom d'utilisateur **analyst** et le mot de passe **cyberops** lorsque vous y êtes invité par Kibana.



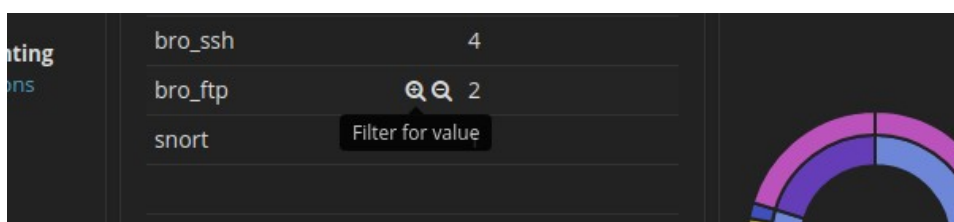
Remarque : si vous avez reçu le message « Your connection is not private », cliquez sur **ADVANCED > Proceed to localhost (unsafe)** pour continuer.

- b. Si la plage de temps correspond aux dernières 24 heures, changez-la en juin 2020 afin que le 11 juin soit inclus dans la plage de temps. Utilisez l'onglet **Absolu** pour modifier la plage de temps.

- c. Dans les résultats affichés, il y a une liste de différents types de données. On vous a dit que le fichier **confidential.txt** n'est plus accessible. Dans la liste Capteurs - Capteurs et services (diagramme circulaire), ftp et ftp-data sont présents dans la liste, comme le montre la figure. Nous déterminerons si FTP a été utilisé pour voler le fichier.



- d. Filtrons pour **bro_ftp**. Passez la souris sur l'espace vide à côté du nombre de types de données bro_ftp. Sélectionnez **+** pour filtrer uniquement le trafic lié au FTP, comme indiqué sur la figure.

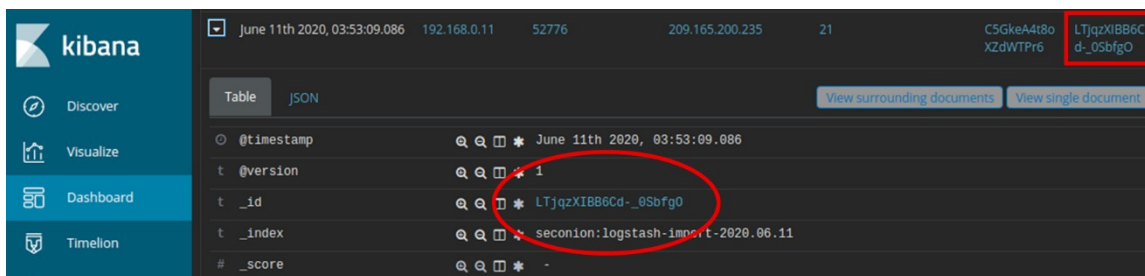


- e. Faites défiler le contenu jusqu'à la section **All Logs**. Il y a deux entrées répertoriées.

Quelles sont les adresses MAC et IP source et de destination et les numéros de port?

- f. Développez et examinez les deux entrées de journal. Dans l'une de ces entrées, le ftp_argument a une entrée ftp://209.165.200.235/./confidential.txt. Consultez également le message dans l'entrée de journal pour en savoir plus sur cet événement.

- g. Dans la même entrée de journal, faites défiler vers le haut jusqu'au champ `_id` d'alerte et cliquez sur le lien.



- h. Vérifiez la transcription des transactions entre l'attaquant et la cible. Si vous le souhaitez, vous pouvez télécharger le pcap et consulter le trafic à l'aide de Wireshark.

Quelles sont les informations d'identification de l'utilisateur pour accéder au site FTP?

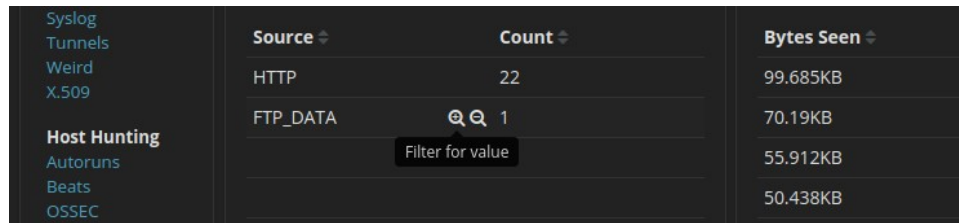
- i. Maintenant que vous avez vérifié que l'attaquant a utilisé FTP pour copier le contenu du fichier confidential.txt, puis l'a supprimé de la cible. Alors, quel est le contenu du fichier? Rappelez-vous que l'un des services répertoriés dans le graphique circulaire est ftp_data.
- j. Accédez au tableau de bord. Sélectionnez **Fichiers** sous l'en-tête de chasse Zeek dans le panneau de gauche, comme illustré sur la figure. Cela vous permettra de consulter les types de fichiers qui ont été enregistrés.



Quels sont les différents types de fichiers? Regardez la section Type MIME de l'écran.

Faites défiler jusqu'à l'en-tête **Fichiers - Source**. Quelles sont les sources de fichiers répertoriées?

- k. Filtrez **FTP_DATA** en survolant l'espace vide à côté du compte pour FTP_DATA et cliquez sur **+**.



Source	Count	Bytes Seen
HTTP	22	99.685KB
FTP_DATA	1	70.19KB
		55.912KB
		50.438KB

- l. Faites défiler vers le bas pour passer en revue les résultats filtrés.

Quel est le type MIME, l'adresse IP source et de destination associés au transfert des données FTP?
Quand ce transfert a-t-il eu lieu?

- m. Dans les journaux des fichiers, développez l'entrée associée aux données FTP. Cliquez sur le lien associé à l'idd'alerte.

Quel est le contenu textuel du fichier qui a été transféré à l'aide du protocole FTP?

Avec toutes les informations recueillies jusqu'à présent, quelle est votre recommandation pour empêcher tout accès non autorisé?