CCNA Cybersecurity Operations v1.0
Évaluation de compétences

Objectifs de l'évaluation

Partie 1 : **collecte d'informations de base** (32 points, 30 minutes)

Partie 2 : **en savoir plus sur l'exploit** (12 points, 20 minutes)

Partie 3 : **détermination de la source des malwares** (36 points, 25 minutes)

Partie 4 : **analyser les détails de l'exploit** (20 points, 25 minutes)

Scénario

Vous travaillez comme analyste en sécurité pour ACME Inc. et vous remarquez plusieurs événements sur le tableau de bord SGUIL. Votre tâche consiste à en savoir plus sur ces événements via l'analyse et la recherche des activités suspectes.

Utilisez Google pour faire vos recherches. Security Onion est configuré pour autoriser l'accès Internet.

Les tâches ci-dessous vous offrent des indications tout au long du processus d'analyse.

Vous serez noté sur les compétences suivantes :

- Évaluer les événements Snort/SGUIL.
- Utiliser SGUIL pour lancer ELSA, Bro et Wireshark afin d'étudier les événements plus en détail.
- Utiliser Google comme outil de recherche pour en savoir plus sur un exploit potentiel.

Le contenu de cette évaluation est issu du site http://www.malware-traffic-analysis.net/. Nous l'utilisons avec l'autorisation du propriétaire que nous remercions pour sa contribution.

Comptes et services en ligne

La partie 5 de cette évaluation s'appuie sur des bases de données en ligne. Vous pouvez créer vos propres comptes gratuits avec ces services, mais vous pouvez également utiliser les identifiants suivants pour vous connecter.

Analyse hybride :

URL : http://www.hybrid-analysis.com

Nom d'utilisateur : **cyops.analyst@gmail.com**

Mot de passe : **cyber0ps**

VirusTotal :

URL : http://www.virustotal.com

Nom d'utilisateur : **cyops.analyst@gmail.com**

Mot de passe : **cyber0ps**

Table d'adressage

Les adresses suivantes sont préconfigurées sur les périphériques réseau. Les adresses sont fournies à des fins de référence.

Appareil	Interface	Réseau/Adresse	Description
Machine virtuelle Security Onion	eth0	192.168.0.1/24	Interface connectée au réseau interne
	eth2	209.165.201.21/24	Interface connectée aux réseaux externes ou à Internet

Partie 1 : Collecte des informations de base

Total de points : 32

Durée : 30 minutes

Remarque : fermez toutes les applications et tous les services superflus pour améliorer les performances de la machine virtuelle.

a. Ouvrez une session sur la machine virtuelle Security Onion avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.

b. Ouvrez une fenêtre de terminal. Saisissez la commande **sudo service nsm status** pour vérifier que tous les services et les capteurs sont prêts.

c. Lorsque le service nsm est prêt, ouvrez une session dans SGUIL avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**. Cliquez sur **Select All** pour surveiller tous les réseaux. Cliquez sur **Start SQUIL** pour continuer.

d. Dans la fenêtre SGUIL, identifiez le groupe d'événements associés à des exploits. Ce groupe d'événements est associé à un seul exploit à plusieurs parties.

Combien d'événements ont été générés par l'exploit complet ? (_____ / 4 pts)

_____

_____

e. Selon SGUIL, quand l'exploit a-t-il commencé ? Quand s'est-il terminé ? Combien de temps a-t-il duré approximativement ? (_____ / 4 pts)

_____

_____

_____

f. Quelle est l'adresse IP de l'ordinateur interne impliqué dans ces événements ? (_____ / 4 pts)

_____

g. Quelle est l'adresse MAC de l'ordinateur interne impliqué dans ces événements ? Comment avez-vous procédé pour le trouver ? (_____ / 4 pts)

_____

h. Quels sont les ID sources de certaines des règles qui se déclenchent lorsque l'exploit sévit ? D'où proviennent ces ID sources ? (_____ / 4 pts)

_____

i. Ces événements vous paraissent-ils suspects ? Semble-t-il que l'ordinateur interne ait été infecté ou compromis ? Expliquez votre réponse. (_____ / 4 pts)

_____

_____

_____

_____

j. Quel est le système d'exploitation exécuté sur l'ordinateur interne en question ? (_____ / 4 pts)

_____

_____

k. Selon les alertes SQUIL, quel est le kit d'exploit (EK) utilisé ? (_____ / 4 pts)

_____

Validation de la partie 1 par le formateur : _____

Points : _____ sur 32

Partie 2 : En savoir plus sur l'exploit

Total de points : 12

Durée : 20 minutes

a. Qu'est-ce qu'un kit d'exploit ? Effectuez une recherche web pour répondre à cette question. (_____ / 4 pts)

_____

_____

_____

_____

b. Le kit d'exploit utilisé est Angler EK. Recherchez rapidement « Angler EK » sur Google pour en savoir plus sur les principes fondamentaux de ce kit d'exploit. Présentez vos conclusions ici. (_____ / 4 pts)

_____

_____

_____

_____

_____

c. Quelles sont les caractéristiques de cet exploit qui permettent de dire qu'il s'agit d'un kit d'exploit ? Donnez des exemples tirés des événements que vous voyez dans SGUIL. Quelles sont les principales étapes des kits d'exploit ? (_____ / 4 pts)

_____

_____

_____

_____

Validation de la partie 2 par le formateur : _____

Points : _____ sur 12

Partie 3 : Déterminer la source du malware

Total de points : 36

Durée : 25 minutes

a. Dans le contexte des événements affichés par SGUIL pour cet exploit, inscrivez ci-dessous les adresses IP impliquées. (_____ / 4 pts)

_____

_____

_____

b. Le message du premier nouvel événement affiché par SGUIL indique « ET Policy Outdated Flash Version M1 ». À quel hôte cet événement fait-il référence ? Qu'implique cet événement ? (_____ / 4 pts)

_____

_____

c. Selon SGUIL, quelle est l'adresse IP de l'hôte qui semble avoir diffusé l'exploit Angler EK ? (**Indice**: consultez la première alerte Angler.) (_____ / 4 pts)

_____

d. À partir de SGUIL, ouvrez la transcription de la transaction. Quel est le nom de domaine associé à l'adresse IP de l'hôte qui semble avoir diffusé l'exploit ? (_____ / 4 pts)

_____

e. Quelles sont les trois applications logicielles dont les vulnérabilités sont généralement ciblées par ce kit d'exploit ? (**Indice**: vous pouvez effectuer une recherche sur le web.) (_____ / 4 pts)

_____

f. Selon les événements SGUIL, quelle vulnérabilité semble avoir été utilisée par le kit d'exploit ? (_____ / 4 pts)

_____

g. Quel est le type de fichier le plus couramment lié à ce logiciel vulnérable ? (**Indice**: vous pouvez effectuer une recherche sur le web.) (_____ / 4 pts)

_____

h. Utilisez ELSA pour recueillir davantage de preuves appuyant l'hypothèse selon laquelle l'hôte que vous avez identifié ci-dessus a diffusé le malware. Lancez ELSA et répertoriez tous les hôtes qui ont téléchargé le type de fichier indiqué ci-dessus. N'oubliez pas d'ajuster les délais en conséquence.

Avez-vous trouvé davantage de preuves ? Si tel est le cas, renseignez-les ici. (_____ / 4 pts)

_____

_____

_____

i. À ce stade, vous devriez savoir si c'est le site répertorié dans la **partie 3b** et la **partie 3C** qui a diffusé le malware. Notez vos conclusions ci-dessous. (_____ / 4 pts)

_____

_____

_____

_____

Validation de la partie 3 par le formateur : _____

Points : _____ sur 36

Partie 4 : Analyser les informations de l'exploit

Total de points : 20

Durée : 25 minutes

a. Les kits d'exploit reposent souvent sur une page d'accueil utilisée pour rechercher les vulnérabilités du système de la victime et pour en exfiltrer une liste. Utilisez ELSA pour déterminer si le kit d'exploit en question a utilisé une page d'accueil. Si tel est le cas, quelles en sont l'URL et l'adresse IP ? Quelle en est la preuve ? (_____ / 5 pts)

Remarque : les deux premiers événements SGUIL contiennent plusieurs indices.

_____

_____

_____

_____

_____

_____

b. Quel est le nom du domaine qui a diffusé le kit d'exploit et la charge utile du malware ? (_____ / 5 pts)

_____

c. Quelle est l'adresse IP qui a diffusé le kit d'exploit et la charge utile du malware ? (_____ / 5 pts)

_____

d. À partir des événements indiqués dans SGUIL, lancez Wireshark et exportez les fichiers issus des paquets capturés. Quels fichiers ou programmes avez-vous réussi à exporter ? (_____ / 5 pts)

_____

_____

_____

_____

Validation de la partie 4 par le formateur : _____

Points : _____ sur 20