Amazoom

Niveau 1

Open Space

41

Retournez moi !

Open Space

99

Open Space

97

Open Space

51

Open Space

8

Open Space

92

Open Space

23

Open Space

83

99 Léa

Bonjour,
Oui, nous avons détecté cela il y a 10 minutes. Tout le service est en alerte car cela semble être une cyberattaque assez violente. Nous sommes en train de vérifier les pistes suivantes :

83 Vérifier ce qui se passe au niveau du serveur principal

92 Relancer tous les serveurs, cela devrait réinitialiser le système

23 Mettre à jour tous les navigateurs web (Safari, Firefox, Chrome …)

41 Salle de réunion

C'est l'effervescence dans l'entreprise ce matin ! Plus de site pour l'une des plus importantes entreprises de e-commerce, c'est plus qu'embêtant ! Avec vos collègues, c'est réunion de crise pour comprendre ce qui se passe !

97 Demander à Léo ce qu'il en pense

99 Appeler Léa de toute urgence

8 Voir avec Yves qui n'est pas encore arrivé

Ce jeu a été conçu par l'équipe du **Centre LEARN de l'EPFL**

Crédit images
storyset.com

8 Petit coup de fil !

Yves : Allo ?
Vous : Bonjour Yves, peux-tu aller sur le site de l'entreprise, s'il te plaît ?
Yves : Heu, je suis en visio, là ... hum, c'est bizarre : le site ne charge pas.
Vous : Mince même de l'extérieur le site ne répond plus !

97 Zut, bon...

51 Quelle drôle d'idée !

Un site n'est pas un logiciel qui s'exécute sur ta machine. Redémarrer l'ordinateur ne changera rien à la disponibilité du site.

97 Retour en arrière...

97 Léo

Lorsque je suis arrivé ce matin, j'ai voulu ajouter les dernières actualités sur notre site. Mais pas moyen de m'y connecter. Notre site web n'est plus accessible. Il faut rapidement rétablir la situation.

99 Contacter rapidement le service informatique

8 Appeler Yves qui doit être en télé-travail aujourd'hui, il pourra ainsi essayer d'accéder au site en dehors de l'entreprise

51 Redémarrer l'ordinateur, on ne sait jamais

83 Vérifier le serveur

Le serveur web de l'entreprise est tombé. D'après les logs, nous avons eu 1 million de connexions en moins d'une minute. C'est une attaque de type DOS, Denial Of Service : On sature un serveur en lui envoyant un volume important de requêtes.

Bravo, vous remportez la clé : Attaque par déni de service :)

Appelez votre enseignant·e pour passer au pochain niveau !

23 Mettre à jour tous les navigateurs web ✕

Même si c'est important de garder à jour ses logiciels et particulièrement les navigateurs web qui sont souvent un vecteur d'attaques, là c'est le serveur qui ne répond plus. Ce ne sont donc pas les clients web qui sont défaillants : c'est du côté du serveur qu'il faut rechercher le problème.

99 Hum, essayons autre chose...

92 Relancer le serveur

Avant de redémarrer une machine, encore faudrait-il diagnostiquer le problème… Parfois, on fait cela sur une machine personnelle, mais un serveur, ce n'est pas la même histoire.

99 Hum, essayons autre chose...

Amazoom

Niveau 2

Data Center

38

Retournez moi !

Data Center

58

Data Center

40

Data Center

3

Data Center

33

Data Center

93

Data Center

43

Data Center

30

58 Sonia (admin sys)

Nous avons subi une cyberattaque qui s'est déclenchée à 4h44 ce matin. Tous les serveurs web sont touchés et nous n'avons plus de présence sur le web depuis cette attaque. Il faut vite trouver les causes et remédier à cette situation !

76 Lançons une vérification des pare-feux

93 Démarrons la laborieuse étude des fichiers de logs...

26 Relançons les serveurs au plus vite !

38 Data Center

Responsable de la sécurité, votre mission est de parer toutes les cyberattaques et aujourd'hui, il y a du travail. Tous les sites sont tombés et c'est une situation de crise pour l'entreprise. Que s'est-il passé ? Comment y remédier ?

58 Faire le point avec Sonia, responsable de l'administration systèmes et réseaux

43 Voir avec Yves des RH pour prévenir tous les collègues

30 Informer Elliot de la réception

Ce jeu a été conçu par l'équipe du **Centre LEARN de l'EPFL**

Crédit images
storyset.com

33 Yves (ressources humaines)

Sonia : Bonjour Yves, on a détecté une activité suspecte il y a 10 jours à 12h57 sur ton poste. Est-ce que tu te souviens de ce que tu faisais à ce moment-là ?
Yves : Heu, il y a 10 jours ? À 12h57 ? J'étais à la cantine.
Sonia : Étrange car nous avons une connexion au data center à ce moment là.

63 Te rappelles-tu d'un évènement particulier ce mardi matin ?

64 As-tu partagé ton identifiant et ton mot de passe avec quelqu'un ?

15 As-tu prêté ta machine professionnelle à une connaissance les jours précédents ?

3 Connexions suspectes au data center

Si l'on élimine les connexions liées aux missions du personnel du data center, nous avons identifié une connexion suspecte. Un collègue des RH s'est connecté il y a 10 jours pendant 27s au serveur du SIRH (Système d'Information des Ressources Humaines) et a produit un plantage de la machine qui a été redémarrée 5min après. Très louche !

33 Appeler Yves pour savoir ce qu'il se rappelle de cet évènement

57 Réinitialiser la machine d'Yves

2 Convoquer Yves pour le licencier

40 Logs : postes de travail

C'est laborieux : plus de 540 postes à contrôler. Il va donc falloir établir une stratégie sinon nous ne trouverons pas assez rapidement la source de l'attaque. Nous avons plusieurs pistes possibles :

44 Étudier les logs des temps de connexion des collègues

3 Chercher les connexions du personnel ne travaillant pas au data center vers celui-ci

28 Chercher les machines infectées par des virus

30 Elliot (réception)

Renvoyer les collègues ne travaillant pas dans le centre de données dès qu'ils se présentent à l'accueil ? C'est bien noté, mais je vais me faire recevoir par ceux qui viennent de loin et vont devoir repartir à peine arrivés.

38 Voyons qui d'autre appeler...

43 Yves (ressources humaines)

Comment ? Il faut informer tous les collègues qu'il faut basculer en télé-travail sauf ceux du centre de données ? D'accord, je m'en occupe tout de suite.

38 Voyons qui d'autre appeler...

93 Filtrage des fichiers de logs

Après filtrage des fichiers, on a identifié une attaque de type DDOS : Distributed Denial of Service, une attaque de déni de service avec des millions de requêtes simultanées provenant de milliers de machines généralement déjà contaminées et formant un botnet commandé par ceux ayant pris le contrôle sur ces machines.

5 Étudier les fichiers de logs des serveurs webs

40 Étudier les fichiers de logs des machines des employés de l'entreprise

81 Étudier les fichiers de logs des pare-feux

Data Center

26

Data Center

44

Data Center

28

Data Center

15

Data Center

81

Data Center

5

Data Center

57

Data Center

64

Data Center

2

28 Anti-virus

Bonne idée ! Sur les 540 postes, seuls 10 postes sont infectés, dont 9 par des virus « classiques » n'ayant pas de graves conséquences. Par contre, le poste d'Yves présente une anomalie qui s'est produite il y a 10 jours. La contamination est probablement partie de ce poste.

40 Peut-être du côté d'Yves alors ?

44 Temps de connexion des collègues

En quoi les temps de connexion des collègues pourraient nous aider dans cette situation ? C'est une fausse piste, concentrez vos recherches sur d'autres logs !

40 Creusons une autre piste...

26 Redémarrage des serveurs !

Avant de relancer les systèmes, encore faut-il savoir ce qui s'est passé. Il faut d'abord établir un diagnostic pour identifier la cause du problème. Si on relance juste les serveurs alors qu'ils sont infectés, rien ne redémarrera correctement …

58 Essayons autre chose plutôt...

5 Distributed Denial Of Service

Les logs des serveurs web confirment une attaque de type DDOS : plus de 700 millions de connexions ont été enregistrées à 4h44. Cela a saturé tous nos serveurs et a provoqué leur plantage sous la charge. Par contre, détail étrange : toutes les requêtes proviennent de notre propre centre de données ! Cela signifie que nous avons été contaminés par un virus et qu'un agent extérieur peut contrôler nos machines. On doit immédiatement bloquer l'accès externe, il faut isoler tout notre parc !

93 Une bonne chose de faite, la suite maintenant !

81 Logs des pare-feux

Hum, c'est confirmé, les pare-feu ont été désactivés à 4h40. Nous sommes devenus vulnérables à d'autres attaques externes à partir de ce moment-là. Il faut nous isoler du web et contrôler l'ensemble de notre parc, pas seulement les serveurs. Il est nécessaire de vérifier également les postes de tous les salariés : l'un d'entre nous a dû participer à la contamination du parc.

93 On progresse :)

15 Prêt de machine

Yves : Prêter ma machine professionnelle ? Non, je suis le seul à l'utiliser. Il y a des données personnelles confidentielles vu mes missions RH. Personne d'autre que moi n'utilise et n'accède à cette machine.
Sonia : Bon, je vais creuser une autre piste.

33 Eliminons cette piste...

2 You're fired !

Mais enfin, vous allez vite en besogne. Nous ne savons pas encore ce qui a pu se passer que vous voulez déjà prendre une mesure aux lourdes conséquences ? Trouver d'abord ce qui s'est exactement passé et ensuite seulement la direction prendra acte pour d'éventuelles décisions aussi graves.

3 Réfléchir avant d'agir !

64 Hygiène numérique

Yves : Non, non, je n'ai jamais partagé mes informations de connexion. Je sais bien que c'est interdit.
Sonia : Ne me donne pas ton mot de passe, mais est-il suffisamment sûr ?
Yves : Oui, il fait plus de 12 caractères et contient des caractères spéciaux.
Sonia : Bon, je vais chercher une autre piste pour cette connexion suspecte.

33 Eliminons cette piste...

57 Réinitialisation du poste d'Yves

Effacer l'ensemble du contenu de la machine d'Yves ? La machine qui est sûrement à l'origine de la cyber attaque ! Cette idée relève presque de la faute professionnelle !!! Au contraire, il faut récupérer cette machine et l'étudier pour découvrir si c'est bien la source de l'attaque …

3 Cherchons plutôt ce qui s'est passé avec Yves...

Data Center

76

Data Center

63

63 Cette drôle de clé USB ?!

Yves : Je crois que c'est ce matin que j'avais trouvé une clé USB dans ma mallette. Mais lorsque j'ai regardé ce qu'il y avait dedans, elle était vide ... je l'ai laissée dans mon tiroir.
Sonia : Ok, nous avons peut-être la source de l'attaque : la clé était sûrement vérolée et en la branchant, elle a pu prendre ton identité pour se connecter au SIRH.

Bravo, vous avez gagné la clé : Attaque par clé USB :)

Appelez votre enseignant·e pour passer au niveau suivant !

76 Activons les parefeux !

Très bonne idée ! Apparemment ils ont été désactivés à 4h40. Voici qui va sécuriser les serveurs de nouvelles attaques. Le pare-feu filtre ce qui passe sur le réseau et bloque les paquets douteux. Il faut maintenant comprendre comment ces derniers ont été désactivés.

Bravo, vous obtenez la clé : Pare-feu :)

58 Bien joué, mais il faut comprendre ce qui s'est passé !