Université de Tlemcen Faculté des Sciences Dept. Informatique	Année universitaire 2016/2017 C. BEKARA bekarach@gmail.com

Contrôle Continu Module Sécurité Informatique L3

1h (Documents et Téléphone non autorisés), CC noté sur 13 points

Exercice I (5.75 pts)

- Pour faire expertiser le niveau de sécurité du réseau informatique d'une entreprise, quel mécanisme est utilisé ?
  R : Audit
- Pour pouvoir contrôler le trafic entrant et/ou sortant depuis/vers le réseau informatique d'une entreprise, quel mécanisme est utilisé ?
  R : Firewall ou Pare-feu
- Suite à une attaque informatique, le serveur email d'une entreprise est saturé (espace stockage) par du courrier spam, lequel des services de la sécurité a été affecté ? justifiez
  R : Le service de Disponibilité, car les utilisateurs du serveur email ne sont plus en mesure de recevoir des emails, et éventuellement d'envoyer leurs emails ou au moins garder une copie des emails envoyés
- Pour que les employés d'une entreprise soient à jour en matière de connaissance des risques, vulnérabilités informatiques, ainsi que les contre-mesures, l'entreprise fait appel à quel mécanisme ?
  R : Formation ou Sensibilisation

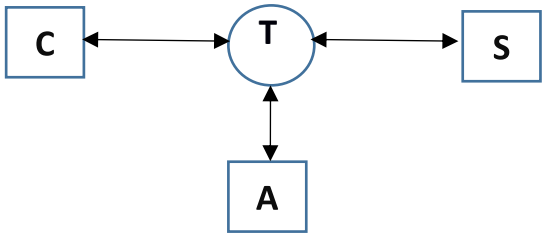
- On suppose que le serveur email de l'université de Tlemcen accorde trois tentatives de connexion pour les utilisateurs (étudiants, enseignants, personnels), au bout desquelles le compte email de l'utilisateur est bloqué pendant 96h. Expliquez brièvement comment ceci peut être exploité pour violer un des besoins en sécurité de l'utilisateur.
- **R** : le besoin affecté est la disponibilité. L'email de la victime (son login) étant le plus souvent connu, l'attaquant n'a qu'à se connecter trois fois successives en fournissant le login de la victime et un mot de passe quelconque
- Classez les pratiques suivantes dans le tableau suivant (vous pouvez indiquer juste les numéros) :

(1) Utiliser le même mot de passe pour accéder à différents services. (**2**) Se connecter à sa machine avec un compte utilisateur à droits restreint. (**3**) Installer des logiciels uniquement depuis le site d'un éditeur de logiciels de confiance. (**4**) Ne pas accorder de l'importance à la mise à jour régulière des différents logiciels. (**5**) activer par défaut l'option exécution automatique depuis des supports de stockage externe. (**6**) Enregistrer les mots de passes dans les navigateurs pour ne pas avoir à les retaper à chaque fois. (**7**) Ne pas verrouiller son poste de travail quand on est loin du poste. (**8**) Ouvrir systématiquement les pièces jointes reçues par email. **(9)** Utiliser des logiciels de chiffrement (ex : bitLockers) pour crypter ses partitions disque.

Pratiques conseillées en matière de sécurité	Pratiques déconseillées en matière de sécurité
2, 3, 9	1, 4, 5, 6, 7, 8

Exercice II (2 pts)

Soit le schéma suivant d'un réseau informatique où **C** : une machine client, **S** : un serveur, **A** : un attaquant, et **T** : un équipement d'interconnexion réseau. Le client se connecte à un service sur le serveur (mail, FTP, etc.) et pour cela doit fournir au préalable un login/ mot de passe.



Q1) Quel est l'utilité du login/Mot de passe ?

R : Sert à prouver l'identité de C (authentifier) auprès de S afin de lui accorder l'accès au service

Q2) On suppose que tous les échanges (trafic) entre C et S se font en clair. Sachant que l'attaquant ne fait qu'écouter le trafic uniquement (n'envoie aucun paquet), pour chacun des configurations suivantes, indiquez les conséquences sur la communication entre C et S (Justifiez) :

A n'envoi aucun paquet donc c'est un attaquant passive n'initiant aucune attaque (il ne fait qu'écouter)

- **T** est un hub
  R : Un hub duplique un paquet reçu vers tous ses ports (machines connectés au hub), par conséquent l'attaquant peut récupérer le mot de passe de C, en plus d'écouter le reste du Traffic entre C et S
- **T** est un switch/routeur
- **R :** un switch, agit comme un commutateur, envoi un paquet reçu uniquement sur le port de la destination (en utilisant l'@ MAC), dans ce cas l'attaquant n'a pas accès aux échanges entre C et S (éventuellement il peut avoir accès au tout premier échange dans le cas ou le Switch ne connais pas encore le port sur lequel est connecté S)
  Un routeur aussi envoi les données uniquement au destinataire (en utilisant l'@ IP), dans ce cas l'attaquant n'a pas accès aux échanges entre C et S

Exercice III (5.25 pts)

Vous disposez d'un compte vous permettant de vous connectez à distance au service de poste en ligne(E-CCP) afin de gérer votre compte postale CCP (consultation, virement, etc.) via le site web https://eccp.poste.dz/ (figure.1).

Figure 1 Site web de connexion au service E-CCP

Q1) On s'intéresse ici au service garantissant à une extrémité la certitude de l'identité de l'autre extrémité. De quel service s'agit-il ? Doit-il être exigé dans un seul sens uniquement (Justifiez) ?

R : Service de Preuve (ou authentification). Non il doit être exigé dans les deux sens, afin de se protéger contre les attaques de type usurpation d'identité. En effet, le client doit s'assurer qu'il fournit ses informations confidentielles (code accès) au vrai serveur eCCP, et le serveur réciproquement doit s'assurer qu'il accorde l'accès au compte eCCP au vrai propriétaire du compte.

Q2) Dans chacun des cas suivants, quels sont les risques encourus et quelle attaque peut être utilisée dans chaque cas, expliquez :

- Cas1 : Par mégarde, sans se rendre compte, vous vous connectez à un site qui ressemble littéralement au site d'accès au service, mais qui n'est pas le vrai site

R : risque de divulgation du code secret du compte client, en plus du numéro CCP, à un attaquant. L'attaque utilisée est le Phishing ou attaque de type site miroir

- Cas 2 : Le service en question est doté d'une vulnérabilité permettant à un attaquant de pouvoir se connecter aux comptes de certains clients existants sans pour autant posséder leurs codes secret, mais uniquement en connaissant leur numéro de compte CCP
  R : risque qu'un attaquant puisse avoir accès et contrôler le compte eccp d'un client victime. L'attaque utilisé peut être de type injection code SQL, pour contourner la phase d'authentification

On suppose maintenant que le service de poste en ligne est exempt de toute vulnérabilité. De même, on suppose que vous êtes un client averti, ne se connectant qu'au vrai site de poste en ligne uniquement, et ne sauvegardant jamais vos codes d'accès aux différents services en ligne sur quelconque support/application.

Q3) Sachant que tous les échanges sur le réseau avec le service E-CCP sont protégés par les services CIP, est-ce qu'un attaquant a un moyen de pouvoir accéder à votre compte en ligne (Argumenter votre réponse) ?

R :

Dans cette partie il faut chercher la faille côté client, car le serveur selon l'énoncé est immunisé (aucune faille) aussi toutes les échanges entre client et serveur transitant sur le réseau sont protégés en CIP donc les attaques de type MITM ou Vol de sessions ne peuvent s'appliquer → il faut noter que côté client l'attaque type phishing ne s'applique plus maintenant (y compris ingénierie sociale, ou empoisonnement dns) pour récupérer son code secret et num ccp donc il est clair maintenant que l'attaquant doit avoir d'une façon ou une autre un accès à la machine du client pour pouvoir récupérer le num ccp et le code secret pour pouvoir les réutiliser pour se connecter ou à la limite avoir accès aux données échangés entre client et serveur avant leur protection en CIP (cas de Man in the Browser , Malware SpyEye) pour pouvoir les manipuler sans être détécté

Oui, et ceci en interceptant mon code d'accès depuis la machine que j'utilise pour se connecter au service eccp, et ceci grâce à un logiciel malveillant de type enregistreur de frappes (keyloggers) ou de type man in the browser. Le logiciel malveillant s'interface entre le clavier et l'OS, où entre l'OS et le navigateur Web qu'utilise le client, afin d'intercepter le code secret d'accès (en plus du numéro de compte CCP)

Question bonus (+1): Quelle est l'utilité du champ numéro **3** du formulaire de saisie (Figure 1) ?

R : ce champ sert à s'assurer que la connexion au serveur provient belle est bien (a été initié) d'un humain et non pas un programme, afin de se protéger contre les différents logiciels malveillants