Projet MSI S2

Présentation 2020

Valérie Ménissier-Morain & Philippe Cadinot & Spiderboy

18 mars 2020

Plan

Présentation générale

Étude du niveau de sécurité et sécurisation d'un système d'information

- Audit en boîte noire du système d'information d'une entreprise
- Organisés en 4 groupes (6 à 7 personnes).
- Multiples vulnérabilités (exploitables ou non) et chemins d'intrusion
- But : Exploitation ET recommandations
- Approche *transverse*, recherche de l'exhaustif

Livrables par groupe de projet

- Un rapport d'audit
- Un support de soutenance

Plan

Infrastructure : le système d'information à étudier

- Une infrastructure par groupe
- C'est un audit en boite noire : vous devez tout découvrir par vous même.
- Pour cela il faut passer la première étape : le serveur *frontal* qui masque tout le reste. Si cela s'avère nécessaire nous verrons si nous débloquons les équipes n'ayant pas réussi à le passer.
- Chaque groupe utilise un serveur *frontal* accessible depuis le réseau de l'UPMC avec une IP publique fournie à chaque groupe.
- Possibilité de demander un *reboot* ou une *restauration* des serveurs de l'infrastructure : envoyer un e-mail à Philippe.
- Le SI utilise divers systèmes d'exploitation
- Équipements réseau

Infrastructure : plateforme physique

- Le système d'information de l'entreprise (S.I.) est simulé
- Chaque groupe disposera de sa propre instance du S.I. accessible par son ip publique :
  - IP publique 132.227.89.21 : groupe 1
  - IP publique 132.227.89.22 : groupe 2
  - IP publique 132.227.89.23 : groupe 3
  - IP publique 132.227.89.24 : groupe 4
- Ces IP sont accessibles depuis `ssh` ou toutes les machines en salles (aucun protocole filtré dans les deux sens).
- Aucun accès direct depuis ou vers l'extérieur (tous les protocoles filtrés).

Infrastructure : accès à vos instances

- Le seul point d'accès à la PPTI est `ssh.ufr-info-p6.jussieu.fr`
- Vous n'êtes pas seuls : surtout en cette période difficile.
- Ne pas lancer d'outils nécessitant d'interface graphique (sur `ssh` ou en salle) afin de préserver la bande passante.
- Si c'est absolument nécessaire répartissez-vous cette tâche au sein du groupe
- Ne pas bloquer ou saturer `ssh` : si vous avez besoin de puissance de calcul 10 machines de la salle 14-15/501 sont restées allumées.
- Vous pouvez utiliser des tunnels cryptés pour accéder depuis chez vous aux plateformes.

Infrastructure : limites des investigations

- Vos investigations doivent se limiter *strictement à votre instance du système d'information simulé*.
- Exploiter une faille de la plateforme (s'il en existe) sera considéré comme un hors sujet.
- Vous ne devez pas porter atteinte à la plateforme.
- Vous ne devez pas porter atteinte au réseau de la PPTI.
- Si vous commettez une erreur, assumez, ce sera mieux pour tous.

Plan

Contexte : l'entreprise cible

- L'entreprise GoldFarma a mandaté votre entreprise (choisissez un nom ;-)) pour effectuer un audit en boite noire de son système d'information
- Le système est en production vous devez donc en tenir compte :
  - il doit rester fonctionnel : les demandes de reboot et restauration seront comptabilisées.
  - vous devez éviter d'affaiblir la sécurité du S.I.
  - une fois l'audit terminé le S.I. doit être à son état d'origine.
- La priorité première de l'entreprise est la confidentialité de ses clients.
- L'audit à pour objectif de mettre au jour l'ensemble de ses vulnérabilités, les possibilité d'exploitation de celle-ci, leur classification. Ainsi que les données critiques/sensibles que vous avez pu exfiltrer afin de mesurer les impacts de l'intrusion. Enfin, elle attend un plan d'action correctif afin de sécuriser l'infrastructure.

Contexte : votre organisation

- Vous êtes mandaté par votre entreprise (trouvez un nom).
- Définissez vos responsabilités / rôles.
- Compte tenu du contexte et tant que ce sera nécessaire il vous est interdit de vous retrouver physiquement.
- Cependant vous devez travailler ensemble au sein de chaque groupe : utilisez toute solution possible de travail collaboratif pour faire des points tout au long de la semaine. Certain permettent le partage d'écran/documents, des conférences audio/vidéo à plusieurs ou en tête à tête : plus ou moins limités en durée (gratuits).
- Sauf déséquilibre de compétence de pentest au démarrage : les groupes doivent travailler indépendamment.
- Définissez un coordinateur pour interagir avec nous si nécessaire.

Plan

Rapport d'audit

- Présentation de l'infrastructure auditée
- Exemple de scénario d'intrusion
- Liste des vulnérabilités rencontrées accompagnées de leur(s) contre-mesure(s) techniques
- Vous devez noter ces vulnérabilités en tenant compte du contexte de l'entreprise
- les informations que vous avez pu ex-filtrer : mesure de l'impact de l'intrusion
- Conclusion d'évaluation du niveau de sécurité de l'infrastructure
- Plan d'action correctif pour sécuriser l'infrastructure
  à court / moyen / long terme

Soutenance

Organisation de la soutenance

- Entre 15 et 20 minutes de soutenance
- 5 à 10 minutes de questions/réponses
- Présentation du travail de chacun
- Présentation du plan d'action correctif

Quand ?

- Date prévue : fin d'après-midi du dernier jour de votre année universitaire
- Date réelle compte tenu du coronavirus ?
- On espère pouvoir le faire en présentiel.