OPPIDA CONSEIL ET EXPERTISE EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Virtualisation et sécurité

Retours d'expérience

Hervé Hosy

Sylvain Pouquet

Agenda

- 2 retours d'expérience abordés
  - Client bancaire : étude de sécurité pour valider un projet de déploiement d'une infrastructure virtualisée de plus de 1000 serveurs
    - ➔ Étude réalisée avant la mise en production
    - ➔ Analyse de risque préliminaire
    - ➔ Recherches et veille en sécurité sur la virtualisation, en particulier sur le produit VMware sélectionné par le client
    - ➔ Tests intrusifs sur plateformes
  - CNES : un cahier d'exigences et de recette pour la mise en œuvre d'une infrastructure virtuelle basé sur le produit VMware
    - ➔ Étude amont

Au sein d'OPPIDA

- Evaluation Critères Communs (ISO 15408)
  - Projet SINAPSE
    - ➔ Evaluation (en cours) EAL5/AVA_VLA.4 d'une solution de virtualisation commanditée par la DGA
- Produits VMware Workstation, Server et ESX
  - Utilisation quotidienne des trois produits
  - Plateforme de test liée à nos activités CESTI et veille sécuritaire
  - Missions d'expertise sécurité pour le compte de clients

1er retour d'expérience

Client bancaire

Client bancaire – Contexte

- Objectifs du client
  - Une plate-forme hébergeant un ou plusieurs serveurs virtuels avec VMware ESX (jusqu'à 1000)
  - Environnement mutualisé multi-clients, multi-métiers, et multi-sites
- Étude demandée
  - Identifier les vulnérabilités potentielles de la future plate-forme
  - Vérifier l'étanchéité des différentes instances VMware
    - ➔ Au niveau réseau, mémoire, I/O...

Client bancaire – Environnement

- VMware ESX 3
  - Environnement multi-clients, multi-sites
  - ESX V3.0.1, Virtual Center, Vmotion
- Aspects continuité d'activité et intégrité très importants
- OS hétérogènes pour les instances
  - Windows NT4,2000,2003
  - Linux RedHat 3, 4 et 5
  - Solaris 10

Client bancaire – Analyse de risque

Exemples de menaces

- Accès non autorisé aux informations contenues dans l'ensemble de la mémoire vive de la plate-forme
- Accès non autorisé aux informations contenues sur le disque dur (fichier d'échange, partition ou disque dur alloués pour une instance VMware)
- Déni de service lié au partage des performances et du temps processeur entre instances VMware
- Accès réseau par décloisonnement inter-instances VMware et avec l'hôte (Guest Isolation)
- Intrusion via les systèmes d'exploitation des instances VMware
- Intrusion via le logiciel VMware (système hôte)

Client bancaire – Analyse de risque

- Vulnérabilités possibles
  - Partage du temps processeur
  - Cloisonnement des flux réseaux
  - Infections virales et codes malicieux
  - Corruption des données en mémoire volatile ou physique
  - Faiblesse de conception de VMware ESX
  - Confidentialité des données
  - Confidentialité des flux réseaux
  - Usurpation d'identité (exploitant, attaquant)
  - Répudiations des actions

Client bancaire – Analyse de risque

- Définition de 43 scénarios de risques
  - Quelques exemples :
    - ➔ Un virus ou un ver informatique ayant infecté l'hôte ESX de la plate-forme de virtualisation VMware pourrait se propager sur des serveurs virtuels de cette plate-forme ou sur d'autres hôtes ESX
    - ➔ Un utilisateur d'un des serveurs virtuels hébergés par la plate-forme de virtualisation VMware pourrait utiliser un outil réseau pour écouter les flux réseau échangés par les autres serveurs virtuels hébergés par cette plate-forme
  - Chemins d'attaques par rapport à l'infrastructure virtuelle
    - ➔ Veille sur la virtualisation et intégration dans les scénarios de risques
- Réalisation des tests intrusifs
  - Sur la base des scénarios élaborés précédemment, vérifier la possibilité de réaliser des attaques, en fonction de la configuration de l'infrastructure virtuelle
  - Proposer des contre-mesures ou proscrire certaines options

Bilan de la mission

- Une grande majorité des failles de VMware touchent la Console de Service (COS) et quelques unes l'hyperviseur
- Failles dans les modules présents sur la COS (Red Hat, Kernel 2.4 pour ESX 3.0)
- Possibilité de configurer l'infrastructure virtuelle VMware ESX de manière non sécurisée, du fait du grand nombre d'options disponibles
- Certaines fonctionnalités pouvant avoir un impact pour la sécurité sont peu, voire pas du tout, documentées

2ème retour d'expérience

CNES

CNES – Contexte

- Objectifs du client
  - Migration d'environnement physique en un environnement virtualisé
  - Implémentation d'une plate-forme VMware ESX 3.5, 3.5i
- Étude demandée
  - Étude amont
  - Cahier d'exigences pour la définition d'une infrastructure virtuelle sécurisée
  - Cahier de recette pour mettre en œuvre la sécurité au sein de l'infrastructure virtuelle

CNES – Cahier d'exigences

Postulat initial

- L'étude s'appuie sur le postulat suivant :
  - ➔ Le cloisonnement des ressources matérielles mis en œuvre par le noyau vmkernel d'ESX est robuste et exempt de faille de type vm-escape (sortie de machine virtuelle)
- Dans le temps, il peut s'avérer que ce postulat initial ne soit plus vérifié.
  Si tel est le cas, un plan d'action devra être élaboré par la SSI du CNES

Catégorisation des exigences

- Exigences liées à la politique de virtualisation
- Exigences liées à l'hôte et à l'infrastructure virtuelle
  - ➔ Sécurité physique
  - ➔ Sécurité logique
  - ➔ Infrastructure virtuelle et des hôtes ESX
  - ➔ Administration de l'infrastructure virtuelle
  - ➔ Composant Virtual Center
- Exigences liées aux instances virtuelles
  - ➔ Système et architecture
  - ➔ Réseau

- Exemples
  - Exigences de sécurité logique
    - ➔ ELO9 - Le protocole iSCSI est interdit au sein de l'infrastructure Virtual Infrastructure du CNES
      iSCSI est un protocole d'encapsulation servant à transporter le protocole SCSI. La sécurité des communications n'est pas implémentée par défaut dans iSCSI ; son utilisation est interdite par défaut au sein du CNES
    - ➔ ELO10 - Les mesures de protection contre le spoofing d'adresse MAC et les transmissions forgées doivent être activées sur le virtual switch sur lequel est connecté le port de la console de service (COS)
      Ces mesures doivent également être appliquées sur le port de la COS
    - ➔ ELO11 - Les mesures de protection contre l'écoute réseau (sniffing) doivent être activées sur le port de la COS, ainsi que sur le virtual switch sur lequel il est connecté

CNES – Cahier de recette

- Pour chaque exigence de sécurité
  - Description d'une ou plusieurs façons de satisfaire à l'exigence
  - Liste des procédures, commandes, options à configurer
  - Mode opératoire pour vérifier l'efficacité de la mesure de sécurité

CNES – Exemple de fiche de recette

R-ELO11	
Rappel exigence	ELO11 - Les mesures de protection contre l'écoute réseau (sniffing) doivent être activées sur le virtual switch sur lequel est connecté le port de la console de service ainsi que sur le port de la console de service.
Pré requis	Accès distant à l'hôte ESX Client Virtual Client Droit Administrateur Virtual Client
Version Vmware	ESX 3.x ☒ ESXi 3.x ☒
Mode opératoire	La vérification de l'exigence ELO11 s'effectue exclusivement depuis un accès administrateur à l'aide du client Virtual Client. L'administrateur se connecte à l'aide du client Virtual Client au serveur Virtual Center qui gère l'hôte ESX. Il choisit le datacenter qui héberge l'hôte ESX à configurer (cf. Figure 10), puis il sélectionne l'onglet Configuration et enfin l'entrée Networking dans le panneau Hardware. L'administrateur entre ensuite dans l'onglet Properties du switch virtuel vSwitch0. La console de service est attribuée par défaut au vSwitch0. Le récapitulatif de la configuration du switch virtuel vSwitch0 est alors affiché. Il doit s'assurer que le paramètre PROMISCUOUS MODE est positionné à REJECT. Si ce n'est pas le cas, il est nécessaire de rentrer dans le vSwitch0 depuis l'onglet Ports, puis choisir l'onglet Security. Enfin, il doit positionner manuellement le paramètre PROMISCUOUS MODE à REJECT L'opération doit ensuite être répétée sur l'entrée service console. Pour cela, l'administrateur entre dans les propriétés de vSwitch0, puis sélectionne le Port du service Console. Il choisit l'onglet Security et positionne le paramètre PROMISCUOUS à REJECT. Un message d'avertissement est présenté à l'administrateur lorsqu'il modifie les propriétés du Port lié au service console.
Résultats attendus	Les paramètres MAC ADDRESS CHANGES et FORGED TRANSMITS sont positionnés à REJECT.

Retours d'expérience sur le produit VMware ESX

Retours d'expérience

- Sécurisation de VMware ESX
  - Whitepapers, quelques guide de renforcements
  - Beaucoup d'information sur les forums communautaires VMware
- Manipulations des options VMware et tests
  - Exemple: Problématique réseau
    - ➔ Par défaut, possibilité d'écoute du trafic si deux instances virtuelles utilisent deux interfaces virtuelles différentes, mais attachés à la même interface physique
    - ➔ Configuration de VLAN différents pour chaque machine virtuelle

Retours d'expérience

- VMware backdoor
  - Nécessité pour l'hyperviseur ESX de communiquer avec les instances virtuelles, afin de récupérer certaines informations
  - Utilisée par VMware avec les VMware Tools
  - Peu de documentation officielle

- Travaux des chercheurs en sécurité
  - Ken Kato sur la backdoor et la façon de l'exploiter
    - ➔ VM Back
  - Joanna Rutkowska, détection d'environnement virtualisé
    - ➔ Red Pill