RS2P – Module d'Introduction à la sécurité informatique

Université Claude Bernard Lyon 1

EXAMEN

NMAP / METASPLOIT

1. Que fait la commande suivante ?
`nmap -sV -p22,2222 192.168.239.42`

2. Les commandes `nmap -O IP_machine_cible` et `uname -a` sur la cible cible ne renvoient pas toujours la même information. Rappelez quel information obtient t'on avec ces commande et pourquoi cela ne correspond pas toujours ?

3. Grace a Metasploit et un de ces exploit vous avez réussi a profité d'un faille pour obtenir un *shell root* sur la machine cible. Qu'allez vous faire pour vous assurer un retour facile sur cette machine ?

4. Sur quels ports peut-on lancer un service HTTP ?

- [ ] Uniquement le port 80
- [ ] Uniquement les ports 80 et 443
- [ ] Uniquement le port 22
- [ ] N'importe quel port disponible

5. Si mon navigateur affiche un « petit cadenas » je reste tout de même sur mes gardes. Que dois-je vérifier avant de donner ou saisir des informations sensibles sur ce site qui semble à première vu sécurisé ?

6. Quel type d'attaque ne peut être déjoué par un antivirus ?

7. Est-ce qu'une backdoor peut se mettre en attente de connexion sur le protocole UDP ?
OUI / NON

DOCKER/CONTENEURS

8. Quelles sont les affirmations vraies sur les conteneurs ? * plusieurs réponses possibles
- Les conteneurs apportent une meilleur sécurité que les VMs
- Le coût en ressource (cpu/ram) de base d'un conteneur est plus faible que celui d'une VM
- L'architecture processeur (x86, arm...) de la machine n'influe pas sur les conteneurs
- Un conteneur démarre en règle général plus rapidement qu'une VM

9. Quelles sont les affirmations vraies sur les images docker ? *
- Une image contient un OS entier (kernel et applications)
- On versionne les images avec des tags
- Les images peuvent être stockées dans des registres
- Les images docker et celles de VM sont interchangeables

10. Je veux faire tourner une bdd mysql (accessible depuis d'autres machines) dans un conteneur, à quoi dois-je faire attention ? *
- Persister les données avec un volume
- Je ne le fais pas, on ne fait pas de BdD dans des conteneurs
- Configurer le transfert de port
- Configurer le redémarrage automatique du conteneur

11. Je veux démarrer un conteneur avec une image nginx, quelle est la commande valide ?
- docker start -d nginx:latest -p 8080:80
- docker init -d nginx:latest -p 8080:80
- docker run -d nginx:latest -p 8080:80
- docker pull -d nginx:latest -p 8080:80

Openstack / Virtualisation

12. Quels types de virtualisation avons-nous effectués avec OpenStack *

- Virtualisation des serveurs
- Virtualisation des architecture x86
- Virtualisation des réseaux
- Virtualisation des systèmes d'exploitation

13. Quelle technique de virtualisation utilise des *namespaces* :

- Noyau en espace utilisateur.
- Isolation.
- Hyperviseur de type 1.
- Hyperviseur de type 2.

14. Openstack fournit un service du type :

- Paas - Platform-as-a-Service.
- Saas - Software-as-a-Service.
- Iaas - Infrastructure-as-a-Service

15. Vous voulez vous connecter sur la machine de votre voisin, pour cela, il faut :

- Utiliser sa clé privée.
- Utiliser sa clé publique.
- Copier votre clé privée dans le fichier authorized_keys.
- Copier votre clé privée dans le fichier known_hosts.
- Aucune de ses réponses n'est correcte.

16. Pour pouvoir se connecter à votre machine avec un mot de passe, il faut : *

- Modifier le fichier /etc/ssh/ssh_config.
- Modifier le fichier /etc/ssh/sshd_config.
- Mettre les arguments PermitRootLogin et PasswordAuthentification à yes.
- Mettre les arguments AllowUsers et PasswordAuthentification à yes.