o

Sécurité du système d'exploitation (Instructions d’examen)

INFORMATIQUE ET SYSTÈMES - ORIENTATION SÉCURITÉ DES SYSTÈMES

CODE UE : IE-IR-B2-SS212-SÉCURITÉ DU SYSTÈME D'EXPLOITATION

Hénallux – Catégorie Technique – 2020-2021

Table des matières

Objectifs

Merci de lire (et relire) toutes les consignes avant de commencer. Durant cette évaluation finale, vous allez :

- Améliorer vos capacités de recherche et de compréhension des concepts en termes de la sécurité des OS.

- Parcourir, manipuler et mettre en œuvre les différents éléments et outils abordés lors de l'ensemble du cours :

    - Part 1 (Domicile): Conception et manipulation des basiques
    - Part 2 (Jour de l'examen): Analyse réflexive et réponses à un formulaire sélectionné sur Moodle
    - Part 3 (Jour de l'examen): Dépôt du rapport sur Moodle

Renseignements pratiques

Comment

A distance et sur Moodle.

Merci de vérifier votre accès aux différents documents et cela AVANT la date fixée de l'examen.

Quand

Préparatif jusqu'au 8 juin

Le mardi 8 juin de 11h à 13h (2h).

Quoi

L'examen consistera en :

- La mise en place d'une infrastructure de travail déterminée (à domicile et sera cotée)
- Un quizz Moodle avec remise du rapport d'exécution des actions effectuées liées à la mise en place de l'infrastructure et entreprises lors du quizz (Actions à clôturer et rapport à poster dans les 2h de l'examen).

La matière

Connaissance des principes pour LDAP et PAM

L'un des trois éléments suivants sera considéré comme sujet principal du quizz :

- Metasploitable 3
- Zabbix
- Powershell

La partie réflexive de sécurité se portera sur ces aspects :

- Reconnaissance
- Enumération
- Scanning
- Gain et maintien des d'accès
- Recouvrement des traces

Les services et vulnérabilités à traiter seront uniquement :

- Servers Web (Apache, Tomcat, IIS)
- SNMP & WMIC
- WinRM & Powershell
- PSEXEC
- SSH & RDP
- FTP & WebDav

Liste des vulnérabilités utilisables pour cet examen :

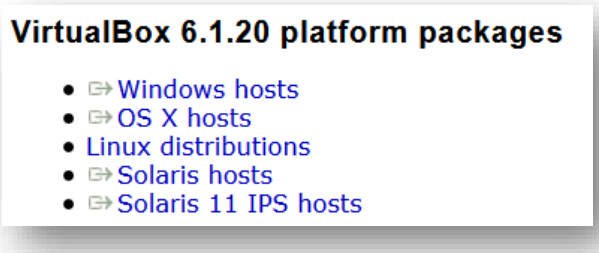
https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities

Tâches à réaliser pour l'examen

Ci-dessous les versions testées pour la mise en place :

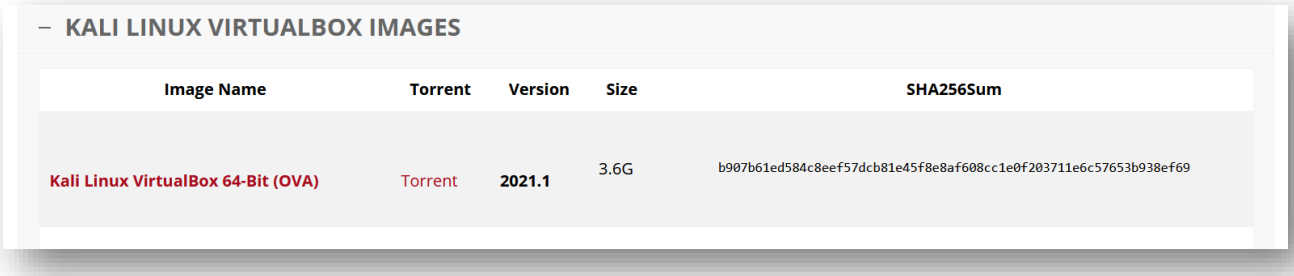
VirtualBox: 6.1.20

https://www.virtualbox.org/wiki/Downloads



KALI Linux : 2020.2 64bit :

https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b

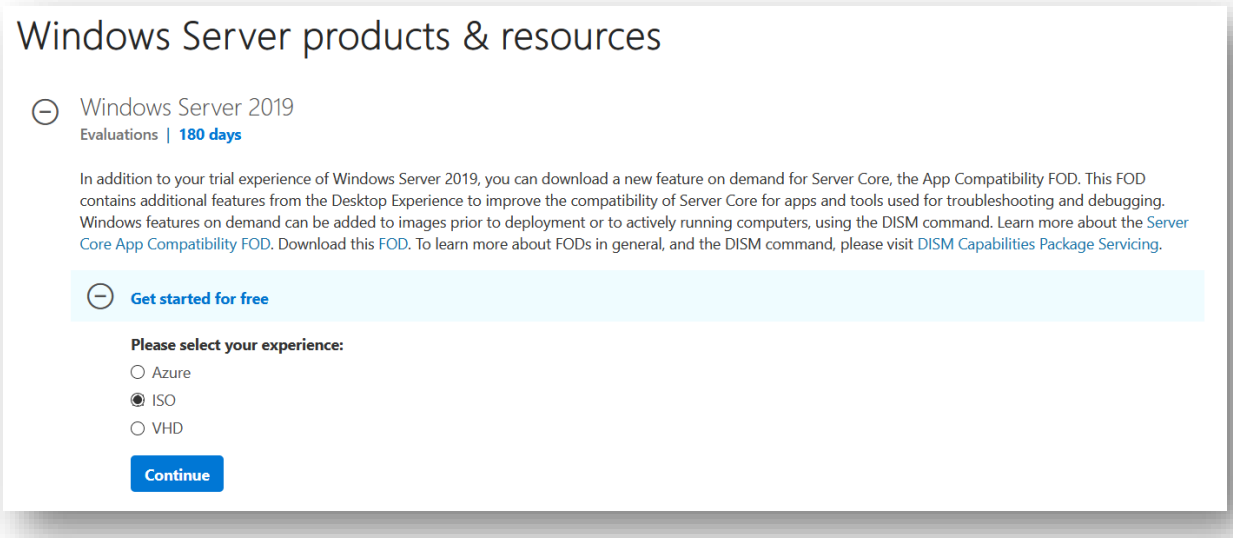


KALI LINUX VIRTUALBOX IMAGES

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2021.1	3.6G	b907b61ed584c8eef57dcb81e45f8e8af608cc1e0f203711e6c57653b938ef69

Windows 2019 Evaluation 180 jours:

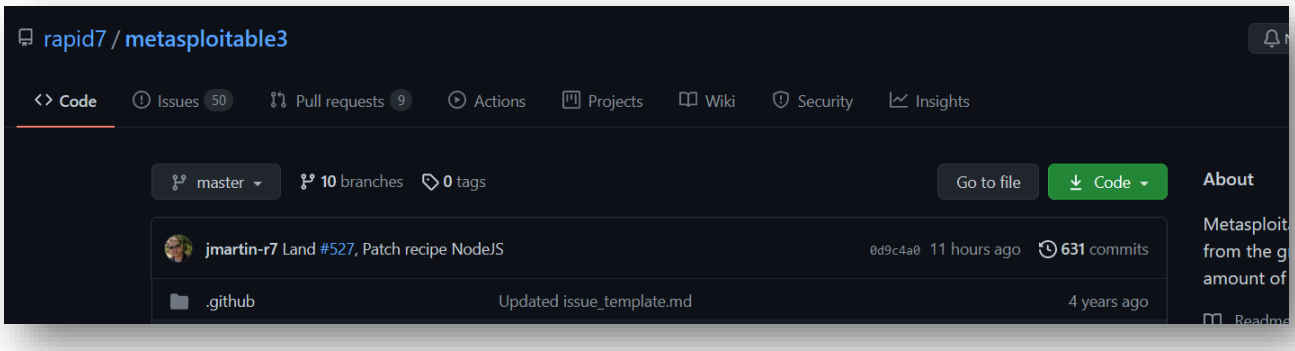
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019



Metasploitable 3 :

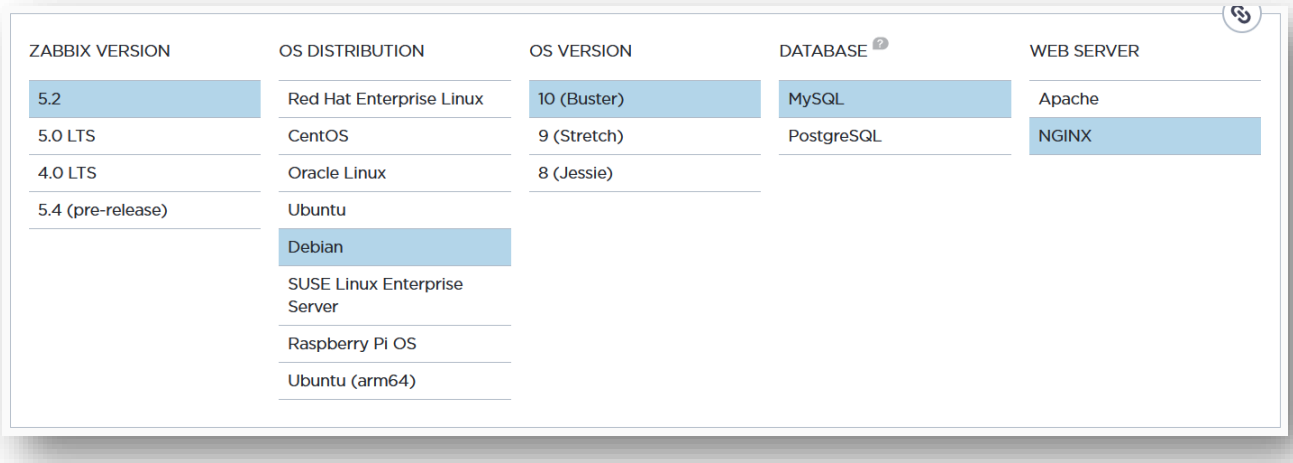
Suivre le HowTo pour l'installation automatisée, ou les vidéos du cours théorique.

https://github.com/rapid7/metasploitable3



Zabbix: 5.2 – Debian 10 – MySQL – Nginx

https://www.zabbix.com/download



Remarques importantes

- Travailler exclusivement avec les mêmes machines virtuelles lorsque que vous faites des modifications de configuration le jour de l'examen.

- Les services des mises à jour sont DÉCONSEILLÉS afin d'éviter une possible perte de temps.

- Il est conseillé de planifier un snapshot et de le tester avant le jour de l'examen.

- Pour une économie de ressources, le système hébergeant doit avoir en permanence 4.5Gb de RAM et 60Go de disque local disponibles.

- Toutes les machines ne seront jamais utilisées en même temps mais doivent être configurées.

- Le travail est à faire individuellement, toute copie venant d'une autre personne sera sanctionnée d'un ZÉRO.

Infrastructure à réaliser

Il vous est demandé de créer l'infrastructure avec les utilisateurs comme mentionnés ci-dessous :

ETUXXXX étant votre ID d'étudiant HENALLUX.

Sur la machine contenant Metasploitable 3 :

Créer un utilisateur simple Local: ETUXXXXXW

Version standard de Powershell

Sur la machine contenant Zabbix :

Utilisateur simple Linux : ETUXXXXXL avec un UID de [1234]

Sur le Windows Server, une AD installée comme suit : FQDN : ETUXXXXXDC.SECUOS.EXAM

NETBIOS AD : SECUOS

Utilisateur dans le groupe des administrateurs : ETUXXXXXADM

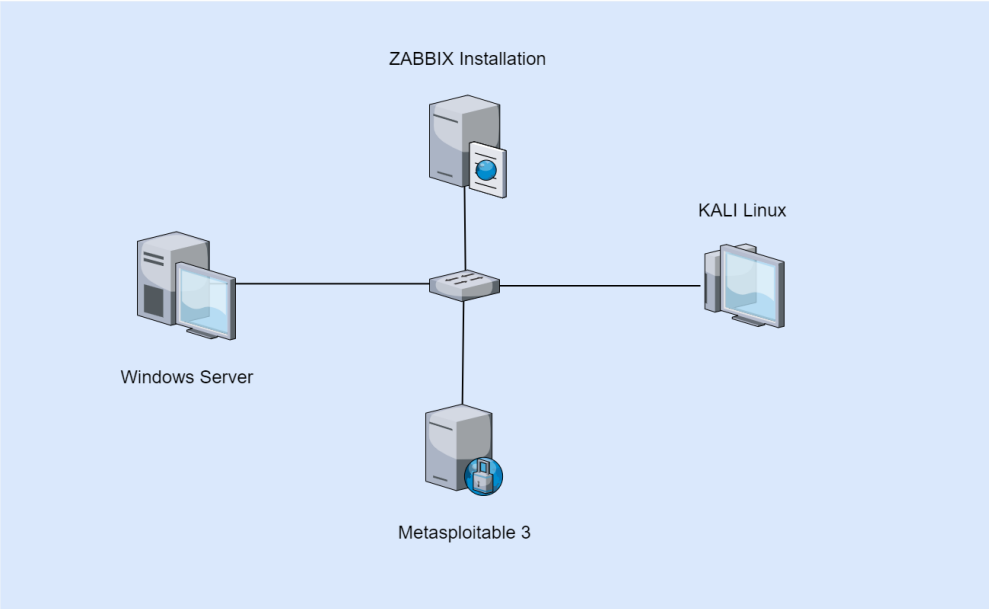
Utilisateur simple AD Windows : ETUXXXXXAD

Version standard de Powershell

Sera principalement utilisée le jour de l'examen.

Password par défaut de tous ces utilisateurs: Tigrou007

Sécurite des OS - Architecture



Travail à réaliser à domicile

Les parties, Metasploitable et Zabbix sont obligatoires et doivent être faites à domicile avec un rapport /!\

Partie Metasploitable :

Exécuter les attaques sur le système adéquat démontrant tous ces concepts de sécurité :

- Reconnaissance
- Enumération
- Scanning
- Gain et maintien des d'accès
- Recouvrement des traces

Sur quatre éléments ci-dessous au choix :

- Servers Web (Apache), Tomcat, IIS)
- Servers Web (Tomcat)
- Servers Web (IIS)
- SNMP & WMIC
- WinRM & Powershell
- SSH
- RDP
- FTP & WebDav

Quand vous exécutez les attaques :

- Faire une capture d'écran de l'état de succès ou non selon la machine.
- Montrer les étapes suivies dans le but de remplir les conditions d'accès ou de succès sur le système adéquat.

Partie Zabbix :

Exécuter une supervision sur le système Metasploitable démontrant ces concepts de sécurité :

- Votre server Zabbix doit tourner en mode sécurisé (Interface Web) tout comme la communication entre agents et serveur se doit d'être sécurisée via TLS.
- La machine Metasploitable doit être monitorée selon un template OS adéquat.
- Superviser les traces de connexion de l'utilisateur ETXXXXX et des super-utilisateurs sur la Metasploitable. Il est évident que vous devez vous connecter sur les machines avec les utilisateurs adéquats pour le fonctionnement.
- Monitorer l'état de statut de tous les services disponibles utilisant :
    - Servers Web (Apache, Tomcat, IIS)
    - SNMP & WMIC
    - WinRM & Powershell
    - PSEXEC
    - SSH & RDP
    - FTP & WebDav
- Générer des sondes personnalisées permettant d'avoir une alerte sur le Dashboard principale de Zabbix lorsqu'une activité ou un service ne répond pas.

Partie Powershell

(Uniquement possible le jour l'examen, selon le quizz):

Elle sera liée soit avec une des 2 parties Metasploitable ou Zabbix faite à domicile.

Ce choix sera fait de manière aléatoire.

La nécessité de la machine Windows Server contenant l'Active Directory sera de mise. Donc, ne pas en négliger la configuration lors de la mise en fonction à domicile.

Documents à réaliser

Pour l'évaluation finale, le jour de l'examen :

- Au préalable avoir mis en place et généré un rapport sur la partie mise en place AD, activités sur Metasploitable et Zabbix.
- Il faudra compléter le quizz proposé.
- Poster un rapport complet, en PDF uniquement, du travail effectué à domicile dans Moodle.

Le rapport contiendra :

- Les preuves de mise en place de l'infrastructure.
    - Copies d'écran faisant apparaître la preuve avec quand cela est possible, votre numéro d'étudiant
    - Une brève explication de chaque copie d'écran
- Les parties du travail concernant Metasploitable et Zabbix.
    - Copies d'écran faisant apparaître la preuve avec quand cela est possible, votre numéro d'étudiant
    - Une brève explication de chaque copie d'écran
- Tout comme les annexes éventuelles des questions demandées ce jour.

La cotation intègre donc :

- Toute la matière du cours pour les actions à réaliser à domicile.
- Un choix aléatoire de quizz qui se basera soit sur Powershell, Metasploitable ou Zabbix. Cela pour le jour de l'examen.

Le rapport est à remettre au plus tard la veille de l'examen !!!

Bon travail à tous.