Cahier des spécifications projet ingénieur

Préparation Olympiade des métiers Cybersécurité

Samuel Benayed et Pierre Sanchez

Tuteur de projet : Thomas Vantroys

SE5-SC 2020/2021

Objectifs

Les compétiteurs doivent savoir procéder à des tests d'intrusion, c'est-à-dire lorsqu'ils simulent des attaques pour rechercher des vulnérabilités dans leurs réseaux avant qu'ils puissent être exploités. Ils doivent être capables de mettre en place un environnement réseau et de le sécuriser. Les compétiteurs doivent être capable de rejouer une capture de l'activité d'un réseau compromis et d'en déduire le scénario d'attaque. Ils devront également être capable d'analyser un réseau afin d'en déduire les failles et les exploiter pour retrouver des mots de passe ou obtenir un accès root.

La compétition aura lieu du 13 au 17 décembre 2020.

Environnement d'entraînement

Pour nous entraîner à toutes les tâches nous aurons besoin d'un environnement particulier :

Nous utiliserons VirtualBox avec les images suivantes :

CentOS 8 :
Packages installés : OpenVPN, FreeIPA

SELinux 2.8 : Installation standard

Windows Server 2016 : Logiciel : BlueHound

Windows 10 : Logiciels installés : Mimikatz, Powershell empire

Kali Linux : Installation standard

Security Onion 16 : Logiciels installés : Kibana, Sguill

Nous allons créer une archive (hébergée sur archives.plil) contenant toutes les machines virtuelles préconfigurées utilisées afin de les mettre à disposition des autres étudiants souhaitant également s'entraîner à ces exercices. Cette archive contiendra l'énoncé des exercices ainsi que les machines à utiliser.

Détails des tâches

I. Installation et sécurisation d'un environnement réseau

- Installation des images disques

Télécharger et préparer tous les systèmes d'exploitation pour la réalisation de nos entraînements et créer les images disques à héberger sur archives.plil. Nous prévoyons différents tests pour optimiser l'espace utilisé sur le serveur.

- Hardening Linux - Remote Logging

Configurer un serveur CentOS (s1) pour qu'il envoie ses logs à distance sur un second serveur (s2), en sécurisant les communications au moyen d'un certificat. Les messages en provenance de s1 doivent être placés dans un dossier tel que /var/log/s1.log
Délai de réalisation attendu finales nationales : 1h15
Délai de réalisation attendu finales internationales : 45 mins

- Hardening Linux - Règles d'audit

Configurer une consignation systématique de toute saisie que pourrait effectuer l'utilisateur root au clavier, quel que soit le mode d'accès au système. Toutes les modifications sur ou dans le dossier /etc doivent être monitorées. Les règles d'audit doivent être "immutable"
Délai de réalisation attendu finales nationales : 1h30
Délai de réalisation attendu finales internationales : 45 mins

- Hardening Linux - VPN

Etablir un serveur OpenVPN (s1) et configurer s2 pour être un client VPN de s1. Vous prendrez soin de tester plusieurs variantes pour établir le VPN : connexion par certificat, par utilisateur/certificat, par user/mot de passe, plusieurs sessions distinctes avec le même certificat.
Délai de réalisation attendu finales nationales : 1h30 mins
Délai de réalisation attendu finales internationales : 45 mins

- Hardening Linux - Sécuriser GRUB

Sécuriser GRUB en y associant des utilisateurs et mots de passe, un utilisateur pourra modifier les entrées de GRUB, l'autre pourra choisir les entrées présentées, mais pas les modifier.
Délai de réalisation attendu finales nationales : 20 mins
Délai de réalisation attendu finales internationales : 10 mins

- Hardening Linux - LUKS

Ajouter une partition au système, et la configurer comme un volume chiffré (via luks), ce volume sera monté de façon persistante dans le dossier /myluks
Délai de réalisation attendu finales nationales : 30 mins Délai de réalisation attendu finales internationales : 20 mins

- Hardening Linux - SELinux

Configurer un serveur FTP (vsftpd) sur un système SELinux
Délai de réalisation attendu finales nationales : 1h15
Délai de réalisation attendu finales internationales : 45 mins

- Hardening Linux - Politique de mots de passe

Appliquer la politique de mots de passe suivante : Les mots de passe doivent contenir au moins 2 Chiffres et 2 Majuscules, et doivent avoir une longueur d'au moins 12 caractères. Aucun utilisateur ne pourra avoir plus de 2 sessions ouvertes, sauf l'utilisateur "lambda" qui aura droit à 5 sessions. Après 4 essais infructueux, un compte sera bloqué pour 5 minutes, un rapport contenant tous les accès infructueux sera envoyé toutes les heures à l'utilisateur root.
Délai de réalisation attendu finales nationales : 45 mins
Délai de réalisation attendu finales internationales: 30 mins

- Hardening Linux - Authentification centralisée

Un serveur d'authentification (s1) est équipé de freeIPA, il assigne des UID qui commencent à l'UID 4000. Les mots de passe expirent au bout de 10 jours, et les 10 derniers mots de passe ne pourront pas être réutilisés en cas de changement de mot de passe. Seul le premier utilisateur créé pourra utiliser ssh pour se connecter sur d'autres systèmes (par exemple depuis le serveur s2 vers s1). Le premier utilisateur dans IPA pourra faire sudo sur la commande fdisk, le second utilisateur pourra faire seulement sudo sur fdisk mais que s'il est sur une troisième machine (s3).

Délai de réalisation attendu finales nationales : 45 mins
Délai de réalisation attendu finales internationales : 30 mins

- Hardening Linux - Partage

Créer un dossier partagé sur s1n et y accéder depuis s2, le dossier sera protégé par krb5p.
Délai de réalisation attendu finales nationales : 20 mins
Délai de réalisation attendu finales internationales : 10 mins

- Hardening Linux - GPG

Créer une clé gpg pour un utilisateur (lambda1) et l'exporter pour un second utilisateur (lambda2). Créer un fichier (secret.txt) avec lambda2, il sera chiffré avec l'export réalisé pour lambda1. Lambda1 doit pouvoir lire ce fichier.
Délai de réalisation attendu finales nationales : 20 mins
Délai de réalisation attendu finales internationales: 10 mins

- Hardening Windows

Connaissance de powershell type 'administrateur' (remote session, WMI, fournisseurs)
Découverte de Mimikatz, bluehound et powershell empire pour auditer une infrastructure Windows Active Directory
Création d'un Lab composé d'un serveur AD et d'un ou deux clients sur lesquels on aura des administrateurs locaux.

Possibilité également de s'entraîner à l'élévation de privilèges sur notre propre lab (exercice biaisé mais cela permet l'assimilation du protocole).

II. Compromission d'un environnement (Red team)

- Digital Forensics

Il faudra être en mesure de mener une live et dead analysis sur des postes soit windows, soit linux. L'objectif de la live analysis est de valider si une attaque s'est réellement déroulée sur un système et de prélever des indices permettant la mise en évidence de celle-ci. L'objectif de la dead analysis est d'analyser les dumps de mémoire et disque afin de retrouver les indices de compromission de l'attaque. Nous disposons de plusieurs outils pour nous entraîner, le site "*Rootme*", la machine virtuelle "*victoria*" de honeynet.org.

- Pentesting

Savoir repérer et exploiter les failles de sécurité d'une machine est un bon moyen d'apprendre à les sécuriser. Il faudra donc savoir réaliser des exploitations de failles classiques telles que l'élévation de privilège, les buffers overflows, les failles XSS et CSRF, pour compromettre des machines linux ou windows et récupérer les droits administrateurs. Nous avons à notre disposition des sites telles que "*Rootme*" et "*hackthebox*" tout deux gratuit permettant de compromettre des machines pour s'entraîner.

- Cryptographie

Certaines données sensibles nécessite d'être cryptés afin que leur récupération soit veines ou difficiles. Il est donc nécessaire de connaître les techniques de cryptages basiques ainsi que les outils/méthodes permettant des les décrypter. Pour s'améliorer dans ce domaine nous pourrons également nous aider de "*Rootme*" ainsi que de tutoriel pour le logiciel "*John The Ripper*".

III. Détection d'intrusion sur un environnement (Blue team)

- Malware analysis

Le reverse engineering est également une composante importante de cette compétition. Plusieurs outils seront à notre disposition telles que ida, ghydra, immunity debugger, GDB, EDB, cuckoo sandbox, nous devrons être capable d'effectuer la rétro ingénierie de malwares simples, et suite à cette analyse, d'indiquer ce que fait ce malware.

- Siem Splunk

Nous devons être capable d'installer un SIEM (Security Information and Event Management) splunk, transmettre à splunk les logs de nos équipements actifs et passifs du réseau.

- Exercice post-compétition

Mise en place d'un Network Service Monitoring (distribution Security Onion) dans la salle E306 de Polytech afin de surveiller l'activité des utilisateurs et de détecter d'éventuelles failles ou diffusion de malwares. Il faudra donc installer un port forwarding vers la machine pour intercepter toute l'activité du réseau et mettre en place des outils de monitoring comme Kibana pour visualiser cette activité et qualifier les menaces potentielles.
Nous serons amené à réaliser un guide d'utilisation de ces outils afin de permettre la prise en main de cette solution après notre installation.
Nous étudierons également différents plans de reprise après sinistre.

Tâches à effectuer et diagrammes de Gantt

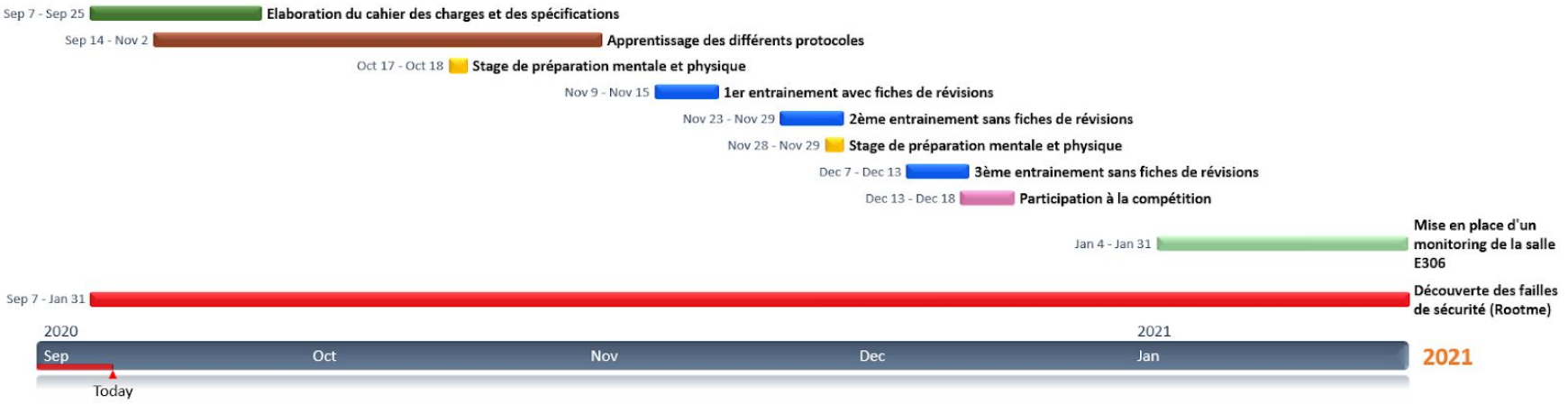
Nous avons choisi de découper notre première partie de projet ingénieur (avant la compétition) en deux parties. La première consistera à étudier des protocoles permettant la mise en place et la sécurisation d'un réseau ainsi que des appareils qui le composent. Tout en faisant des fiches de révision sur le côté afin de pouvoir retrouver aisément des informations de configuration. La deuxième partie consistera à s'entraîner à refaire ces tâches le plus précisément et le plus rapidement possible. Pour ce faire nous avons choisi de faire un tableau excel nous permettant de stocker nos temps et ainsi comparer nos performances avec les anciennes session. Cela nous permettra également de savoir sur quelle partie nous devrons nous concentrer d'avantage. En parallèle de toutes ces tâches nous devons également nous entraîner à la compromission de machine ainsi que la recherche de pièces cachées sur celle-ci. L'apprentissage des différentes failles de sécurité et le reverse engineering de malware nous permettra également de progresser dans ces tâches.

Travail à réaliser :

Protocole a maîtriser	Temps théorique à maitriser	1er entrainement (avec fiche)	2ème entrainement (sans fiche)	3ème entrainement (sans fiche)
Hardening Linux - Remote Logging	1h15m			
Hardening Linux - Regles d'audit	1h30m			
Hardening Linux - VPN	1h30m			
Hardening Linux - Securiser GRUB	20m			
Hardening Linux - LUKS	30m			
Hardening Linux - SELINUX	1h15m			
Hardening Linux - Politique des mots de passe	45m			
Hardening Linux - Authentification centralisee	45m			
Hardening Linux - Partage	20m			
Hardening Linux - GPG	20m			
Hardening Windows - Installation windows server	Pas de référentiel			
Hardening Windows - Configuration réseau	Pas de référentiel			
Hardening Windows - Creation et configuration de l'AD	Pas de référentiel			
Hardening Windows - GPO	Pas de référentiel			
Hardening Windows - Data Collector	Pas de référentiel			
Cisco - Mise en place des équipements réseaux	Pas de référentiel			
Cisco - Configuration des équipements réseaux	Pas de référentiel			
Cisco - Sécurisation des équipements réseaux	Pas de référentiel			
SecurityOnion - Mise en place d'un NSM	Pas de référentiel			
SecurityOnion - Utilisation des ressources d'analyse de données	Pas de référentiel			

Tâches à maîtriser le mieux possible

Malware Analysis
Forensic Windows/Linux
Initiation aux différentes failles de sécurité (Rootme)


Sep 7 - Sep 25
Elaboration du cahier des charges et des spécifications
Sep 14 - Nov 2
Apprentissage des différents protocoles
Oct 17 - Oct 18
Stage de préparation mentale et physique
Nov 9 - Nov 15
1er entrainement avec fiches de révisions
Nov 23 - Nov 29
2ème entrainement sans fiches de révisions
Nov 28 - Nov 29
Stage de préparation mentale et physique
Dec 7 - Dec 13
3ème entrainement sans fiches de révisions
Dec 13 - Dec 18
Participation à la compétition
Jan 4 - Jan 31
Mise en place d'un monitoring de la salle E306
Sep 7 - Jan 31
Découverte des failles de sécurité (Rootme)
2020
2021
Sep
Oct
Nov
Dec
Jan
2021
Today