Cahier des charges projet ingénieur

Préparation Olympiade des métiers Cybersécurité

Samuel Benayed et Pierre Sanchez

Tuteur de projet : Thomas Vantroys

SE5-SC 2020/2021

POLYTECH LILLE

Université de Lille

Région Hauts-de-France

Vue d'ensemble

Afin de préparer l'olympiade des métiers en Cybersécurité, ce projet consiste en la sécurisation de la salle E306 en déployant différents outils, notamment pour le Network Security Monitoring. Vous devrez également étudier différentes optimisation de la sécurité au niveau des équipements réseaux.

Une seconde partie, consistera à réaliser des réponses à incidents en analysant le trafic réseau et en réalisation des opérations de digital forensics sur les binaires récupérés.

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.

Grandes étapes

I. Installation et sécurisation d'un environnement réseau

- Mise en place et sécurisation des équipements réseaux (Cisco)
- Hardening Linux
- Hardening Windows Server and Active Directory

II. Compromission d'un environnement (Red team)

- Digital Forensics
- Pentesting
- Cryptographie

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

- Mise en place d'une distribution Security Onion
- Exploitation de Splunk, Kibana
- Découverte des Next Generation FireWall Fortinet et Palo Alto
- Entraînement au Reverse Engineering (analyse de malware)

Post-Compétition (Janvier 2021)

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. Cette distribution offre également la possibilité de rejouer des scénarios d'attaque.
On peut imaginer l'intégration de cette tâche dans la maquette SE comme nouveau chapitre dans le module de Sécurité Réseau.

Tâches à effectuer et diagrammes de Gantt

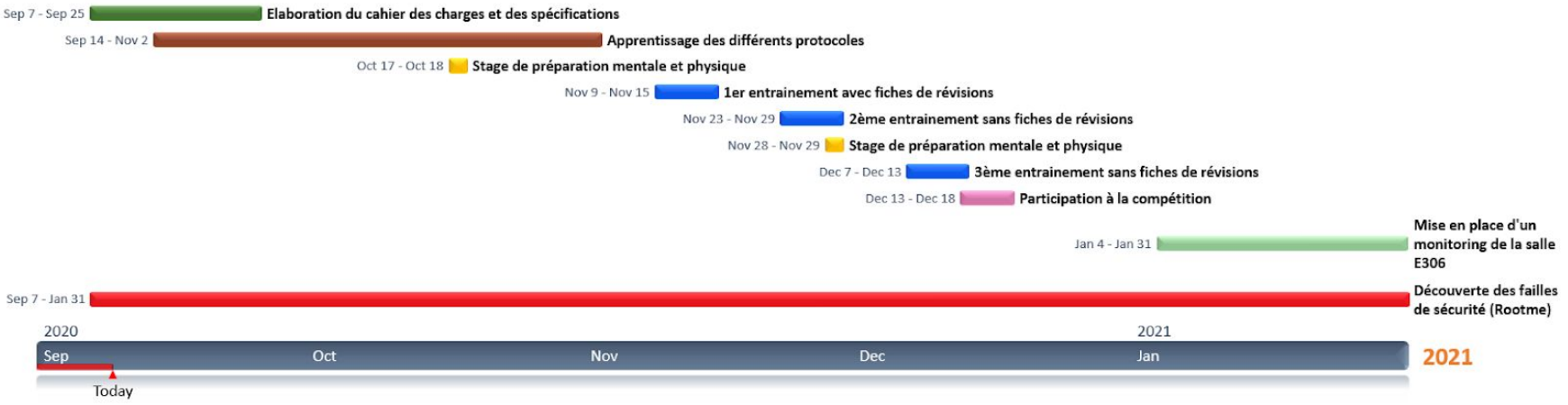
Nous avons choisi de découper notre première partie de projet ingénieur (avant la compétition) en deux parties. La première consistera à étudier des protocoles permettant la mise en place et la sécurisation d'un réseau ainsi que des appareils qui le composent. Tout en faisant des fiches de révision sur 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