Sécurité et réseaux

Compte rendu de projet

Victor BONIN

Sur ce projet d'attaque réseau, mon rôle a été plus théorique que technique. Je me suis surtout renseigné sur le concept de l'attaque, son histoire, et les failles qu'elle implique. Cela m'a permis de découvrir les failles potentielles historiquement liées aux serveurs web et les moyens développés pour répondre à ce type d'attaque.

Si le Malicious File Upload n'est plus une attaque couramment utilisée de nos jours, elle a été bien plus importante et dangereuse il y a quelques années. Aujourd'hui, l'immense majorité des frameworks à jours sont suffisamment stables pour ne plus être vulnérable à ce genre d'attaque, mais elle reste un classique intéressant à connaître et à comprendre et dont certaines parties (par exemple l'élévation des privilège) restent d'actualité.

Concernant les moyens de contrer l'attaque, je retiendrai la vérification du type du fichier, via l'extension ou via des fonctions php comme getimagesize() permettant de s'assurer de la conformité du fichier uploadé, la configuration du firewall pour vérifier les requêtes sortantes permettant le reverse shell, ou encore la restriction des droits dans les dossiers où sont uploadés les fichiers.

Finalement, j'ai trouvé le TP enrichissant car il permettait de découvrir par nous même des méthodes récentes non seulement théoriquement mais en plus d'expérimenter l'attaque, ce qui permet de bien mieux en retenir les concepts. Je regrette néanmoins qu'une séance supplémentaire n'aie pas été mise en place afin de permettre une meilleure synchronisation du groupe et un accompagnement par les enseignants.

Mathieu POURBAIX

Pendant ce TP j'ai participé aux choix de l'attaque, en effet ayant une forte affection pour le développement, les failles de sécurité que peut connaître un serveur web dus au code de l'application sont un domaine qui m'intéresse. Pendant la conception, concentré sur les autres PLD j'ai eu moins l'occasion d'implémenter moi même l'attaque mais j'ai pu m'intéresser au concept et aux outils que le groupe a utilisés. Ainsi j'ai pu m'intéresser à l'alternative plus simple qu'offre vagrant sur des outils plus modernes mais aussi plus complexe tel que Docker.

D'un point de vue apport personnel, j'ai pu apprendre beaucoup sur l'importance de toujours garder en tête pendant le développement de n'importe quel projet l'aspect sécurité de l'application. Des réflexes simples tel que la consultation régulières des bases de données d'exploit et l'utilisation d'outils maintenus. En effet, cela peut éviter simplement de mettre en péril toute la sécurité d'un projet à cause d'une faille déjà connue.

Romain GOUTTE-FANGEAS

Pendant ce TP, j'ai effectué un travail de recherche afin de pouvoir valider les étapes de l'attaques et construire un diaporama en accord avec l'attaque réalisée. J'ai pu tester l'attaque afin de valider les étapes et l'installation des logiciels. Je n'ai eu que peu de temps pour participer à la construction des machines virtuelles à cause des autres PLD en parallèle, ce que je regrette, mais j'ai pu aborder tous les concepts en testant cette attaque.

Ces démarches m'ont permis d'apprendre beaucoup sur ce domaine, notamment sur les exploits et les manières d'exploiter des failles de sécurité. J'ai pu voir que des nouveaux exploits sont publiés régulièrement sur internet, et sont corrigés au fil du temps. L'attaque que nous avons réalisé est donc obsolète car les technologies ont été mises à jour, mais cela reste intéressant pour découvrir les concepts qui sont derrière et participe à notre culture informatique.

Matthieu Valvin

Durant ce projet d'attaque d'un serveur vulnérable, j'ai tout d'abord effectué un travail de recherche afin de déterminer vers quel type d'attaque nous allions nous diriger, quitte à prendre un certain nombre de connaissances sur des notions qui ne seront pas exploitées pour le projet final.

J'ai eu une montée en compétence assez significative sur ma vision générale du monde de la cybersécurité en générale. J'ai pu apprendre et exploiter mes connaissances sur de nombreuses technologies web. Pour ce qui est de l'attaque proposée dans le rendu final, mon rôle je suis resté assez éloigné des travaux de mise en place à proprement parlé. En effet, il a été décidé, pour des raisons d'efficacité et afin de respecter les deadlines des différents projets, que les tâches d'implémentations serait réparties.

J'ai cependant retenu la grande puissance et personnalisation de Vagrant qui permet de créer des environnements personnalisés et adaptés, ce qui est plus qu'utile dans le cas de l'implémentation de TP de cybersécurité. De plus j'ai trouvé ce TP enrichissant car il permet d'aborder le sujet de la cybersécurité sous un angle nouveau.

Paul-Emmanuel SOTIR

Ce TP m’a permit d'en apprendre plus sur comment mettre en place une attaque réaliste de bout en bout et prendre mieux conscience de la vulnérabilité de certaines technologies web ou de l’OS.
Ce projet a également été l'occasion de découvrir diverses technologies de réseaux, sécurité et de devop, comme MetaSploit, Zap, Chef ou Vargrant.
Malheureusement, je n'ai pas eu l'occasion de beaucoup contribuer à l'élaboration de l'attaque étant donné la répartition des rôles qui m'a amené à travailler majoritairement sur le PLD Comp.
Cependant, le projet de cybersécurité auras clairement une influence sur mes futurs choix devOps, notamment concernant les efforts pour s’assurer que les diverses technologies nécessaires pour la sécurité d’un serveur soient à jour et réputées sûres.