Bilan attaque RFI - SERE

Bilan personnel Baptiste Dubarry

1) Configuration et mise en place des machines virtuelles

Bien qu'ayant compris les principes mis en oeuvres pour la configuration et le déploiement des machines virtuelles, je n'ai pas participé à cette phase du projet. Vagrant est un outil puissant qui nous permet de déployer des machines virtuelles préconfigurées mais cependant volumineux.
J'ai pu néanmoins effectuer les premiers tests de déploiement et pu modifier et détailler la procédure de configuration pour la rendre le plus claire possible.

2) Exploitation d'une vulnérabilité via l'upload de fichier

Ne m'étant jamais intéressé à la sécurité informatique auparavant, je me suis longuement documenté sur les "exploits" RFI en suivant plusieurs tutoriels afin de comprendre le fonctionnement global.

J'ai ensuite testé sur l'environnement qui était préparé (serveur web vulnerable + attacker) et j'ai pu de nouveau déterminer certains bugs et permettre leur résolution.

Malgré la vulnérabilité volontaire de notre serveur web, la simplicité du script.php uploaded qui nous permettait d'exécuter n'importe quelle commande shell directement depuis le serveur m'a surprise.

3) Découverte des payload et des générateurs

J'ai pu, grâce à notre attaque, découvrir et me familiariser avec des outils extrêmement puissant comme Metasploit qui sont incontournables dans le domaine de la sécurité informatique.

Dans notre cas, nous avons utilisé ce framework pour nous générer un payload python servant à initialiser un reverse shell. Je ne connaissais pas le concept du reverse shell et son utilisation, même si je n'ai pas pu me pencher en détail sur le code généré par Metasploit (payload ou même l'utilisation du reverse_tcp) j'ai pu appréhender les notions générales.

4) Privilege escalation

Cette dernière partie a été réalisée relativement tardivement comparé aux autres. Durant nos différentes recherches (RFI, LFI, Metasploit etc..) j'ai sans cesse vu les termes de "Privilege escalation" revenir. Notre attaque étant globalement fonctionnel nous nous sommes dit qu'il pourrait être intéressant d'implémenter un privilege escalation.

Après de nombreuses recherches nous avons réussi à trouver un exploit sur le kernel Linux utilisé par la VM de notre vulnerable web server ! Nous avons été en mesure de modifier un exploit trouvé il y a moins de 2 semaines afin de l'intégrer dans notre attaque.

Ce privilege escalation nous a permis d'obtenir un remote shell avec les privilèges root ce qui signifie le contrôle complet du web server. L'utilisation d'une faille aussi récente et l'adaptation à notre attaque a été réellement passionnante.

5) Conclusion

Les deadlines des autres PLD approchant énormément, je n'ai pas participé à la mise en place de l'environnement (vagrant, CDK, Berkshelf etc..) ni à la découverte des vulnérabilités RFI. Cependant j'ai pu jouer le rôle de testeur afin de détecter les bugs, le manque de clarté dans certaines explications. En me documentant et en effectuant un vrai travail de fond j'ai pu participer à la découverte, à la modification et à l'intégration de la partie Privilege Escalation.

Cette attaque, en tant que novice, m'a permis de me rendre compte de la puissance des attaques et des vulnérabilités existantes et de me plonger dans un monde inconnu et passionnant.