POC sur une payload pour la faille blue

EternalBlue : Vulnérabilité SMBv1 dans Windows

Yann BINDIKA SANDOU

SOMMAIRE

I. INTRODUCTION

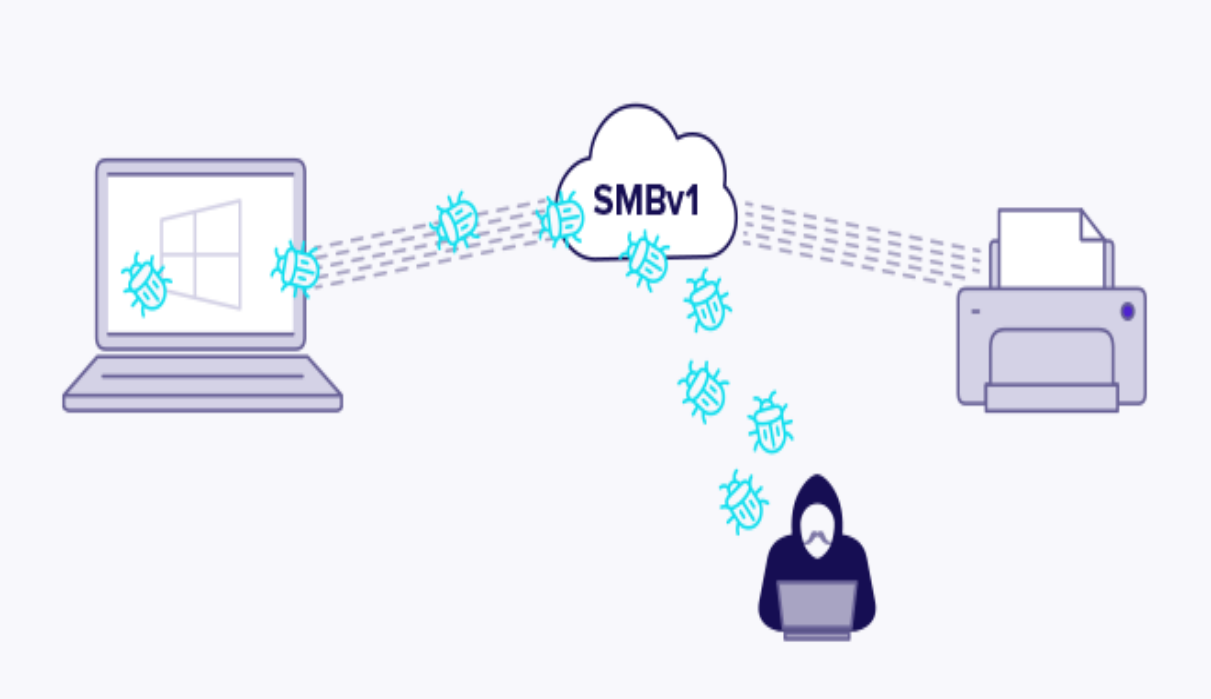
Bonjour,

Je m'appelle Yann BINDIKA et j'ai 25ans. Après l'obtention de ma licence pro en réseau et télécommunications j'ai décidé de faire une formation en alternance en Administration d'infrastructure sécurisé. Je suis en alternance à Iroise Bellevie qui est une entreprise qui gère des Ehpad et résidences services seniors.

Mon sujet porte sur un POC sur une payload pour la fail Blue. En effet, le choix de se sujet porte sur diffèrent paramètres tels que la sensibilisation à la sécurité informatique, l'impact historique mais je pense que ce qui m'a le plus motivé c'est son impact historique qui ramène à la cybersécurité qui reste aujourd'hui un domaine ultra important en informatique.

Cette faille informatique avait pour objectif initial était l'exploitation de la vulnérabilité des systèmes Windows par la NSA. Cependant, cela prend une tout autre tournure lorsque le Groupe des pirates Shadow Brokers l'utilise dans la propagation des logiciels malveillants tel que Wannacry ou Petya.

Schéma du fonctionnement d'EthernalBlue



Voici une liste de quelques vocabulaires utilisés dans ce sujet :

SMB v1: Server Message Block

Payload : un code qui s'exécute sur la cible une fois celle-ci compromise par un exploit

Exploit : Script/programme conçu pour utiliser une faille présente dans le logiciel ou un service

Msfconsole : Console de ligne de commande de Metasploit

RHOST : Remote Host ou l'hôte cible ou écoutée

LHOST : Listener Host ou l'hôte d'écoute

CVE : Common Vulnerabilities and Exposures ou dictionnaire publique relatives aux vulnérabilités de sécurité.

CONTRAINTES

Cette fail n'est plus une assez grande menace aujourd'hui mais reste le toujours pour certains systèmes non patchés Windows. À cet effet, voici un tableau récapitulatif pour ce qui est des contre-mesures à prendre face à cette menace.

Appliquer les correctifs de sécurité
Désactiver le Protocol SMBV1
Mise en place d'un pare-feu
Faire de la segmentation du réseau
Faire la surveillance du trafic réseau

Ressources :

https://www.slideshare.net/kandelrc/eternal-blue-vulnerability?from_action=save

https://notamax.be/pentest-metasploit-et-faille-eternalblue/

CONCLUSION :

En conclusion, nous avons exploré le sujet d'EternalBlue, une vulnérabilité informatique qui a eu un impact considérable sur la sécurité numérique et la cybersécurité mondiale. Initialement découvert comme un outil de cyberespionnage par la NSA, EternalBlue a été divulgué publiquement, conduisant à des attaques de grande ampleur telles que l'attaque Wannacry OU NotPetya.

Cette vulnérabilité a mis en lumière les conséquences dramatiques qu'une faille de sécurité peut engendrer, allant de la perturbation des services essentiels à des pertes financières massives pour les entreprises touchées.

La leçon à retenir d'EternalBlue est que la sécurité informatique est un enjeu crucial dans notre monde numérique en constante évolution.