MOHAMMAD **MUFTI**

Senior Penetration Tester chez ZENDATA

Comment j'ai repris un contrôleur de domaine sur lequel étaient installés SentinelOne et FortiWeb Client.

Cette histoire raconte comment ZENDATA et moi avons réussi à prendre le contrôle complet d'un domaine lors d'un Blackbox Pentest interne.

Comme d'habitude, nous avons passé en revue les listes de contrôle que nous avions - la plupart des attaques ont été bloquées par SentinelOne et FortiWeb, depuis le dumping de hashs, en essayant de réaliser un mouvement latéral. La vérification des partages SMB sur le DC a montré que le partage CertEnroll était ouvert avec un accès en lecture. L'énumération des certificats sur le contrôleur de domaine nous a montré qu'il y avait des vulnérabilités dans ESC1, ESC4 et ESC8. Les consultants de ZENDATA ont été en mesure d'exploiter pleinement l'ESC1 et de prendre le contrôle du domaine en exploitant l'autorité de certification « DC01-ca ». Cette exploitation a pu être réalisée en utilisant une machine non connectée au domaine avec des identifiants d'utilisateur de domaine valides, grâce à un outil appelé « Certipy ».

Nous avons ensuite ajouté notre propre ordinateur « ZENDATA_computer » en utilisant les informations d'identification de l'utilisateur pentest « zendata » via le service LDAP sur le contrôleur de domaine. Pour ce faire, nous disposions d'un quota d'ajout de 100 ordinateurs (tout utilisateur connecté au domaine disposait des mêmes autorisations que nous) - nous l'avions vérifié à l'aide de netexec (version plus récente de CrackMapExec CME).

Nous avons ensuite demandé l'autorité de certification « DC01-ca » et le modèle en utilisant le nouvel ordinateur que nous avions ajouté à l'autorité de certification «ZENDATA_computer », ce qui a abouti à l'enregistrement du fichier administrator.pfx localement sur notre machine. Nous avons ensuite converti ce fichier administrator.pfx en un certificat et une clé.

La transmission du certificat et de la clé nous a donné un accès administrateur complet via le service LDAP. Nous avons donc ajouté l'utilisateur « ZENDATA » au groupe d'administrateurs de domaine et d'utilisateurs de bureau à distance, ce qui nous a donné un accès complet aux contrôleurs de domaine primaire et secondaire.

Des attaques telles que DCSync peuvent être réalisées à l'aide d'un outil appelé «Impacket-Secretsdump ». Il permet le dumping de toutes les machines et de toutes les informations d'identification des utilisateurs, ce qui donne lieu à une prise de contrôle complète du domaine - PTH (Pass-The-Hash). Il peut être utilisé pour se connecter à n'importe quelle machine du domaine.

> "Nous avions un accès complet aux contrôleurs de domaine primaire et secondaire.
>
> Mohammad MUFTI
> Senior Penetration Tester chez ZENDATA

Always in movement to protect

notre équipe.