Rapport Sécurité des Annuaires

Félix Bezançon et Matthieu Jan - Info2

1.Tools

- rpcclient
- crackmapexec
- Mimikatz
- gpp-decrypt
- Enum4Linux
- polenum

Ip de l'AD : 192.168.1.234

Ip d'une machine : 192.168.1.221

2. Déroulement de l'audit

Nous allons ici présenter comment nous avons effectué l'audit de l'AD qui nous était fourni. Nous présenterons les étapes successives en expliquant leur intêret.

2.1 Entrée sur l'AD

Objectif

Afin d'obtenir une vision des éléments constituants de l'AD, comme la liste des utilisateurs ou les politiques de mots de passe, il nous faut un point d'entré.

Actions

Nous avons commencé par essayer d'entrer sur l'AD afin de récuperer des informations de bases. Pour cela, nous nous sommes d'abord connecté anonymement (`user = '' passwd = '''`). A partir de là, nous avons pu decouvrir l'existence du compte 'testad', dont nous avons deviné le mot de passe, 'testad'.

Tools

- rpcclient, pour tester simplement les entrées possibles
- Enum4Linux, pour récuperer les informations disponibles en anonyme

Recommendations

- Voir 3.1

2.2 Récuperation d'un utilisateur

Objectif

Pour pouvoir poursuivre, il nous faut la liste des utilisateurs, eventuellement des groupes,

mais surtout les politiques de mots de passe. Pour cela, il nous faut l'accès à un compte avec plus de privilèges.

Actions

Nous avons énumeré, depuis le compte 'testad', la liste des utilisateurs avec leurs informations, et plus particulièrement leur description. Deux comptes sautent au yeux :

- Le compte k.ren, parce que la description est "mdp=kylo"
- Le compte m.surik, parce que la description est "password**123"

Si le compte k.ren ne donne pas de résultat (parce qu'il est désactivé, mais nous le verrons plus tard), le compte m.surik lui est disponible et nous pouvons nous connecter avec, récuperant ainsi plus d'informations que le compte de test, dont les politiques de mots de passe.

Tools

- Enum4Linux pour récuperer la liste des utilisateurs.

Recommendations

- Voir 3.2

2.3 Politique de mots de passe

Objectif

Afin de savoir s'il est possible d'utiliser des méthodes de bruteforce , et/ou de découvrir si les mots de passe ont une durée indeterminée, nous avons analysé la Politique de mots de passe

Actions

Avec le compte de m.surik, on peut obtenir la politique de mots de passe.

Il se trouve, bien que les longueurs soient insuffisantes (3 caractères),qu'elle est relativement adapté contre le bruteforce. En effet, après 5 tentatitives, le compte se bloque pour 10 minutes.

Typiquement, tester sur chaque compte les 10.000 mots de passe les plus utilisés prendrait un mois environ (ce qui n'est dans l'absolu pas très long), mais qui bloquerait tout les comptes en permanence, et donc devrait attirer l'attention. De plus, les mots de passe expirent après 1 an.

Tools

- crackmapexec --pass-pol

Recommendations

- Voir 3.3

2.4 Compromission de l'Administrateur local

2.5 Vol de Credentials via l'Admin local

2.6 Utilisation du compte helpdesk

2.7 Ouverture

3. Résultats de l'audit

3.1 Compte de test en prod

3.2 Description avec des informations sensibles

3.3 Politique de mot de passe