Windows Saldırı Teknikleri

Öncelikle bir saldırı nasıl yapılır? Bu saldırlar nedir?Bu saldırılara karşı alınann önlemler(sıkılaştırmalar)nedir?
Sürekli Karşımıza çıkabilecek Saldırırları

Windows Sistemelere Yönelik saldırı ,Tespit ve Savunma yöntemleri önem kazanmaya başladı.Günümüzde kurumların sistemlerinde Windows işletim sistemini tercih etmesi ve Active Directory teknolojisini kullanarak yönetiyor olması bunu konunun ne kadar önemli hale geldiğini göstermektedir.

Bahsedeceğim Saldırı çeşitleri

Mimikatz
DCSYNC Saldırıları
Pass the Hash
Golden Ticket
Silver Ticket
Kerberos
Powershell Saldırıları

1)Mimikatz

Windows sistemelerde Issas.exe prosesinde erişilmesi ve bu parolaları açık metin şeklinde ele geçirilmesini sağlayan bir araçtır.
Peki bu Issas.exe nedir diye bakarsak; Windows sistemlerde kullanıcı adı ve parolanızı girdiğinizde güvenlik politakasını ve bu politikayı uygulamaktan sorumlu olan exe devreye girer işte bu proses sürecidir.
Bu Mimikatz ile neler yapabiliriz diye baktığımızda öncelikkle Mimikatz'in Atak vektörlerine bakmak daha doğrudur.
*__Pass The Hash Saldırısı__ →Windows sistemlerde sunucu veya istemciye yapılan saldırılardır.Bu saldırılar sonucunda ise parolalarımıza yapılan saldırı tekniğidir.
*__Golden Ticket__ →Domain Controllere DC e yapılan saldırı tekniğidir.Saldırı sonucunda erişimin gerçekleşmesinden sonra yapılan saldırıdır.Tüm kullanıcıların parolaları alınabilir tehlikelidir
*__Silver Ticket-Kerberos__ → Silver ticketta Golden ticket giibi bir geçiş bileti ancak Kerberos kimlik dentimi mekanizması kullanır Ticket denilen biletler üzerinden gerçekleşir ataklar.
*__Pass the Ticket__ →Aynı mantığa denk gelip Silver Ticket-Kerberos ataklarının birleşiminden oluşur.

Mimikatz İnternal Sızma testlerinde ve Recktim saldırılarında kullanılır.Temel olarak yaptığı iş passwordleri memmoryden açık olarak ele geçirmektir. Burda dikkat edilmesi gereken en önemli noktalardan bir tanesi Yüksek yetkiyle kullanılabilen kullanıcılar üzerinde çalıştırabiliriz.Yani yüksek

yetkide çalıştırdığınızda aşağıdaki gibi okumaya yetki verir Mimikatz.

- **privilege::debug**
- **sekurlsa::logon password**

```
PS C:\mimikatz> C:\mimikatz\x64\mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Jun 18 2017 18:46:28
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 21 modules * * */

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 36128278 (00000000:02274616)
Session           : RemoteInteractive from 6
User Name         : jeff
Domain            : JEFFLAB
Logon Server      : JEFFLAB-DC01
Logon Time        : 09/07/2017 21:06:43
SID               : S-1-5-21-2490182989-4136226752-3308112936-1103
        msv :
         [00000003] Primary
         * Username : Jeff
         * Domain   : JEFFLAB
         * NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
         * SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
         [00010000] CredentialKeys
         * NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
         * SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
```

Kullanıcı oturum açmak için kullanıcı adı ve parolasını giriyor.Gelen bilgilerüzerinden Isas prosesi aracılığıyla sem bilgileri veritabanına gönderilir.Gelen verilerle veritabanındaki bilgiler karşılaştırılır.Eğer kullanıcı adı veya parola ısas parolasını hashli bir tutarak veritabanına kaydeder.Bizde Mimiktazi kullarak Isas.exe servisis üzerinden bir güvenlik açığı oluşturur hahleri ele geçirmiş oluruz.

2)Pass The Hash Saldırısı

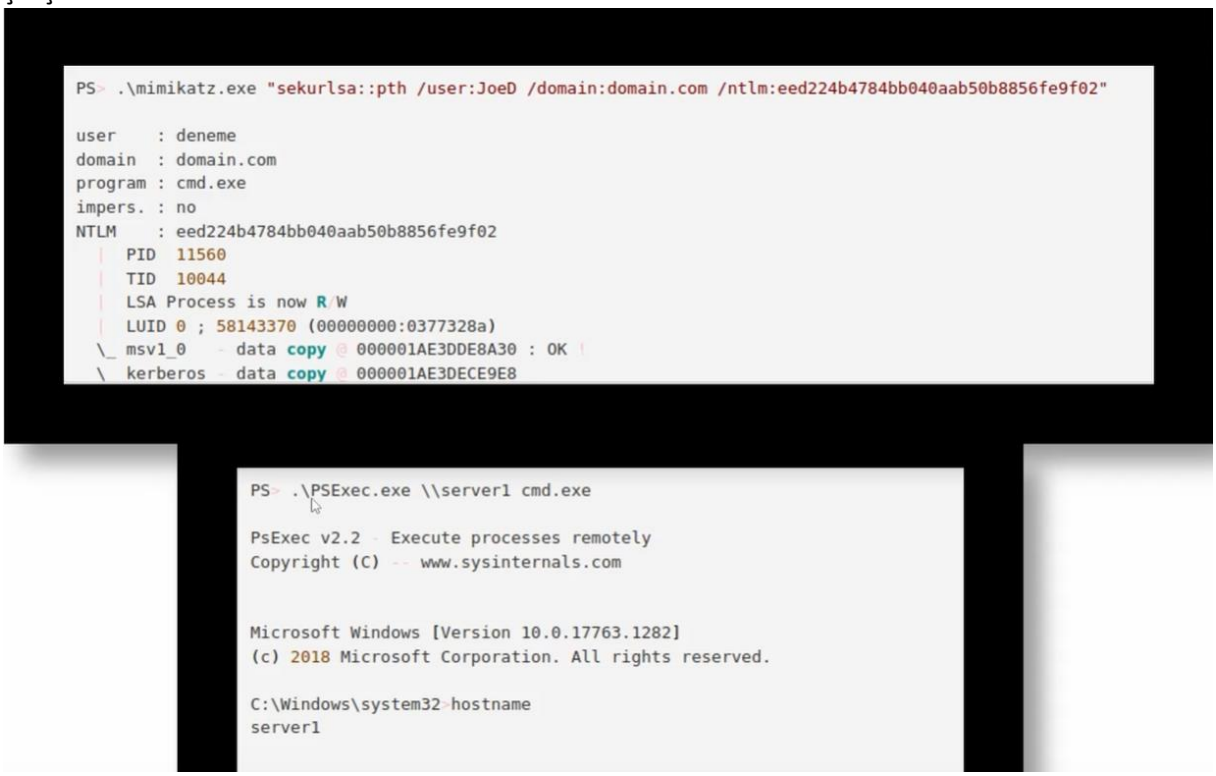
Windows sistemlerde sunucu veya istemciye yapılan saldırı sonucunda parola veya LM/NTLM hashlerinin parola yerine geçirilen Hashler kullanılarak,kimlik doğrulama işlmei yapılmasına **"pass the hash"**saldırı tekniği denir.Aslında bu işlem kimlik bilgi hırsızlığı olarak adlandırılabilir.
Örnek üzerinden devam edelim Saldırgan sisteme bir şekilde sızmayı başarıyor.V ebu saldırı sonucunda ağda yerleştikten sonra parolaları ele geçirmek için birkaç yol var bunun en yaygın olanı ısas.exe dosyasıdır.Bu çıktıda ise ısas.exe den çıkan hashları göstermektedir.

```
PS> .\mimikatz.exe "privilege::debug" "log passthehash.log" "sekurlsa::logonpasswords"

Authentication Id : 0 ; 302247 (00000000:00049ca7)
Session           : RemoteInteractive from 2
User Name         : deneme
Domain            : DOMAIN
Logon Server      : DC1
Logon Time        : 09/07/2020 10:31:19
SID               : S-1-5-21-3501040295-3816137123-30697657-1109
        msv :
         [00000003] Primary
         * Username : deneme
         * Domain   : DOMAIN
```

Saldırgan bu atakta kimlik doğrulaması yapmak için çalınan parola hashini kullanarak bir saldırı yapıyor.Bu örnekte bu cmd.exe yi başlatmak için kullanılan çalınan parola hashini kullanmak için

yapılan işlemler görülmekte .Saldırgan aslında edindiği yetkileri kullanarak PsExec adında bir araç kullanabilir.Bu araç ile Windows sistemlerde uzaktan kontrolü sağlayan bir araçtır.Sistem haklarıyla çalışabilir.

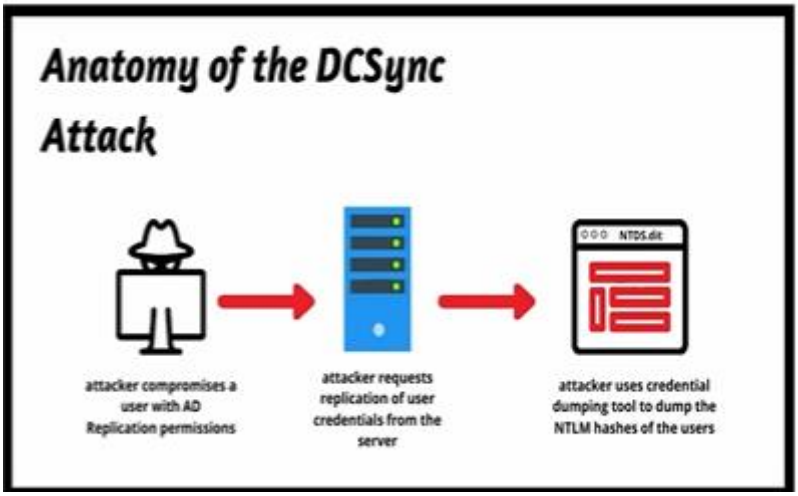


Pass The Hash Saldırısından korunma Yöntemleri

Kullanıcı yetkileri denetlenmeli
Şirket çalışanlarınıza güvenlik konusunda farkındalık eğitimi vermelisiniz
SBM servisi kontrol edilmelidir
Kritik sistemlerde 2FA uygulanmalıdır.
Log kayıtları kontrol edilmelidr
Yüksek yetkili hesaplar son kullacıya bağlanılmamalıdır.

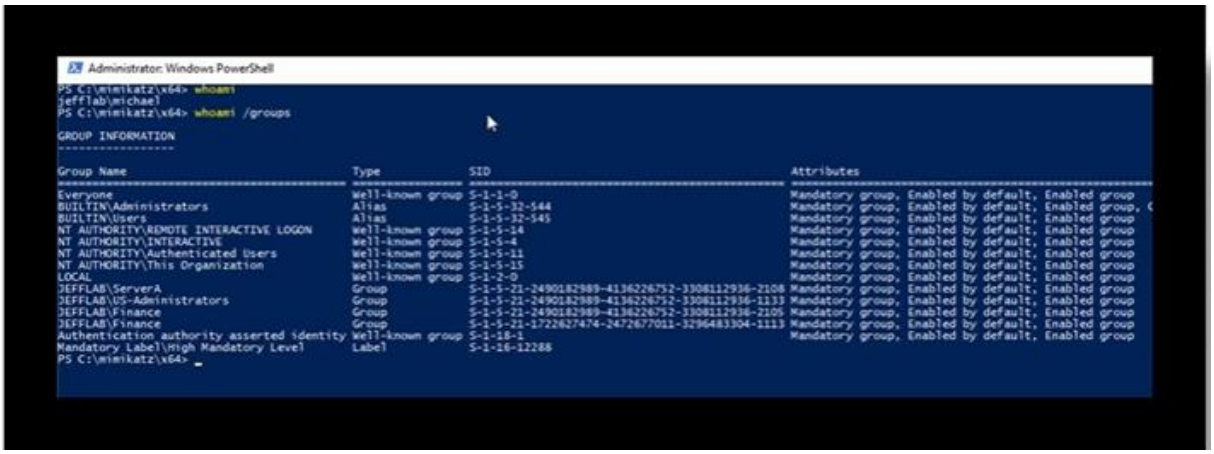
3)DCSYNC Saldırısı

DCSync saldırısı domain controller gibi davranması nedeniyle diğer domain controllerdan kullanıcı adı ve parola bilgisini elde etmek için kullanılan bir saldırı tekniğidir.

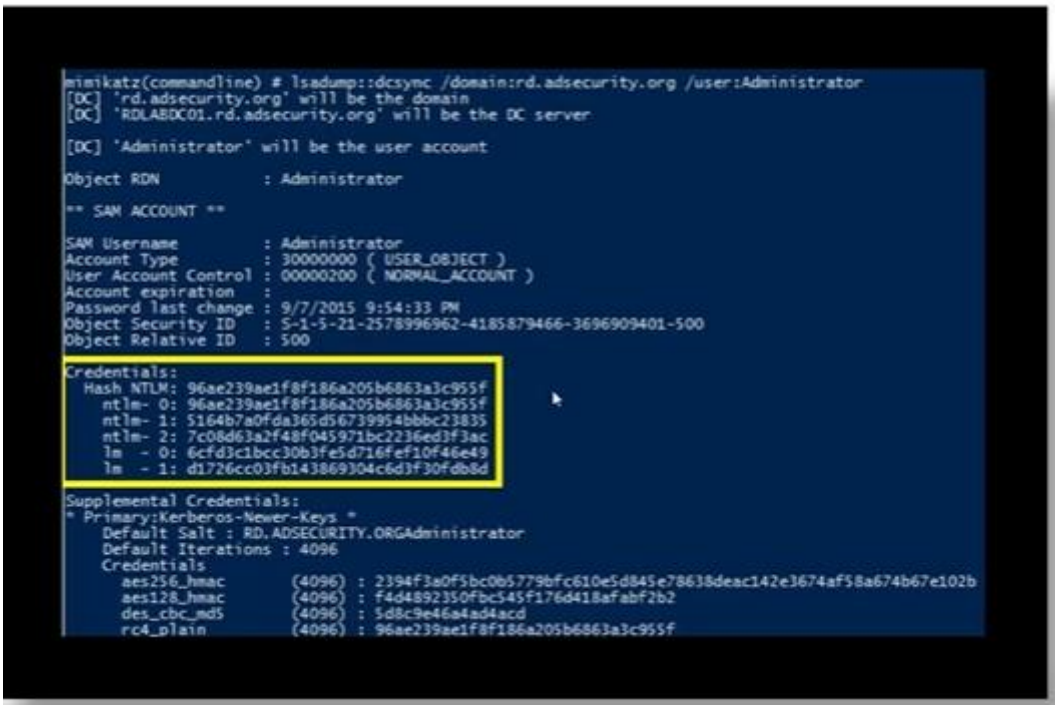


Saldırı süreci→ saldırgan domain controller taklidi yapmak için yetkili gruplara dahil olan bir

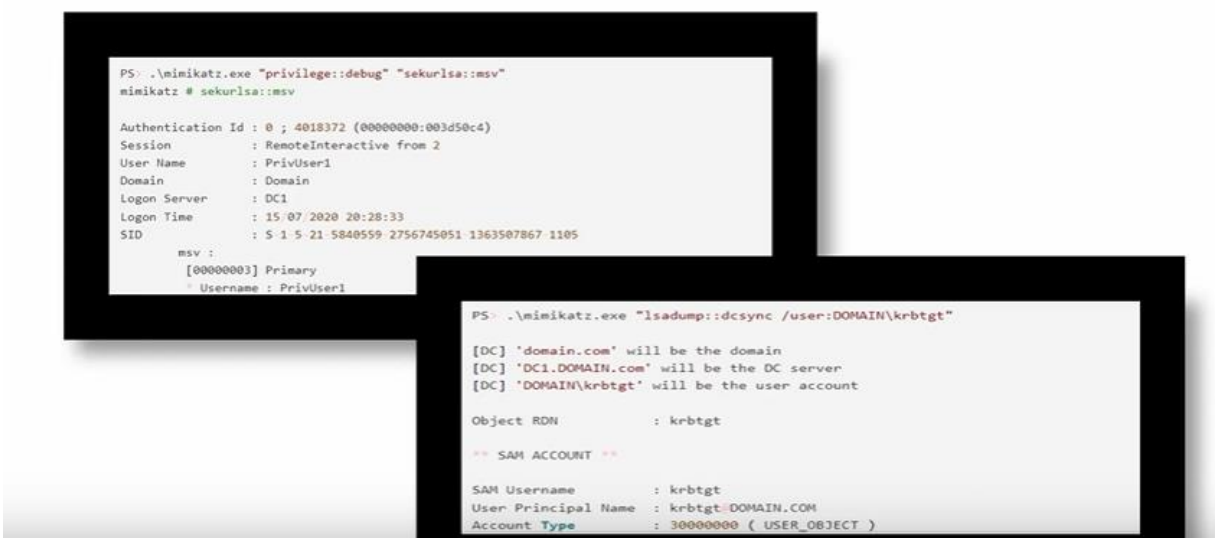
kullanıcıya ihtiyaç duyar.Active Directory yapısısında bulunan kullanıcıların parola bilgisini ele geçirmek için mimikatz aracılığı ile DCSynnc saldırısı gerçekleşmiş olur.
Burada kullanıcının yetkili gruplara dahil olup olmadığı kontrol edilmiştir



Burada mimikatz üzerinden bir dcsync saldırısı gerçekleştirilmiştir.Eğer siz tek bir kullanıcıının parola ve hash bilgilerini elde etmek istiyorsanız buradaki saldırı tekniğini kullanabilirsiniz.



Hedef sistem üzerinde mimikatz çalıştırıldıktan sonra saldırıya devam edimiş.kullanıcı hedef alınmış ve bu kullanıcıya yeni bir şifre üretilmeye çalışılmıştır.



Golden ticket saldırısı örneğidir.Parola hashine sahip olmuş kullanıcının ve Active directory üzerinde sınırsız erişim hakkı kazanılıyor.

4)NTDS.dit Saldırısı

NTDS.dit saldırısı Windows sunucu sistemlerinde default olarak active directory verilerinin depolandığı veri tabanı dosyasıdır.NTDS.dit dsyası içerisinde kimlik bilgileri gibi kritik verileri barındırır.Bu veriler saldırganların ele geçirmek istedikleri bilgiler olduğundan dolayı NTDS.dit önemlidir.

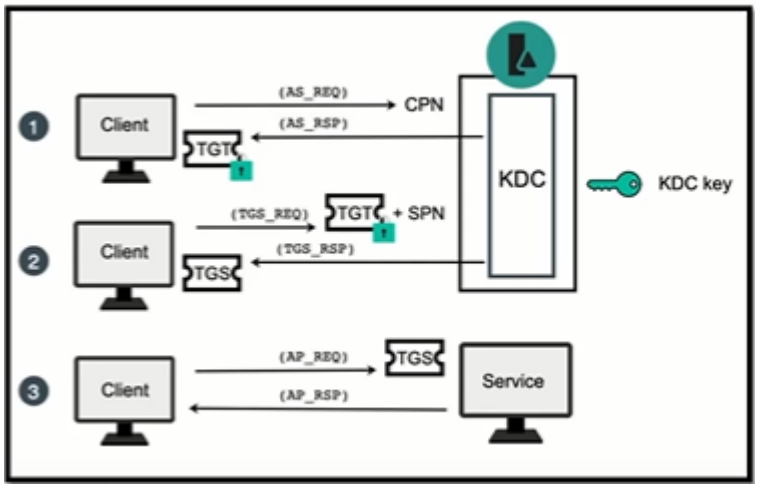
5)Golden Ticket Saldırısı

Kerberos:

Kerboros güvenli olmayan bir ağ üzerinde haberleşen kaynaklarının bilet mantığını kullanarak kendi kimliklerini tanıtarak iletişim kurmalarını sağlayan bir kimlik doğrulama protoklüdür.

KDC(Key Distrubution Center) Kerberos kimlik doğrulamasıda kullanılan bir servistir.Authentication Service ve Ticket Granting Service olmak üzere iki bölümden oluşur.

TGT(Ticket Granting Ticket) Kerberos bileti veren servistir.Domain Logon işlemlerinde kullanılır.



Öncelikle bir client düşün bu bilgisayara kullanıcı adı ve şifresi ile giriş yapıyor.Kullanıcı adı ve şifre şifrelenerek Kdc kısmına gelirler.Burda birkaç işleme tabi tutulur.Authentication Service gelen bu kullanıcı adını kontrol eder(veritabanında olup olmadını kontrol eder)Sonrasında KDC tarafından burda daha güvenli bir iletişim için ticket üretilmeye başlanıyor.ve sonrasında üzertilen tgt şifreleerek client tarafına gönderiliyor.Clientte tgtler daha güvenli bir iletişim için tekrar KDC kısmına gönderiliyor.Döngü bu şekilde devam ediyor.

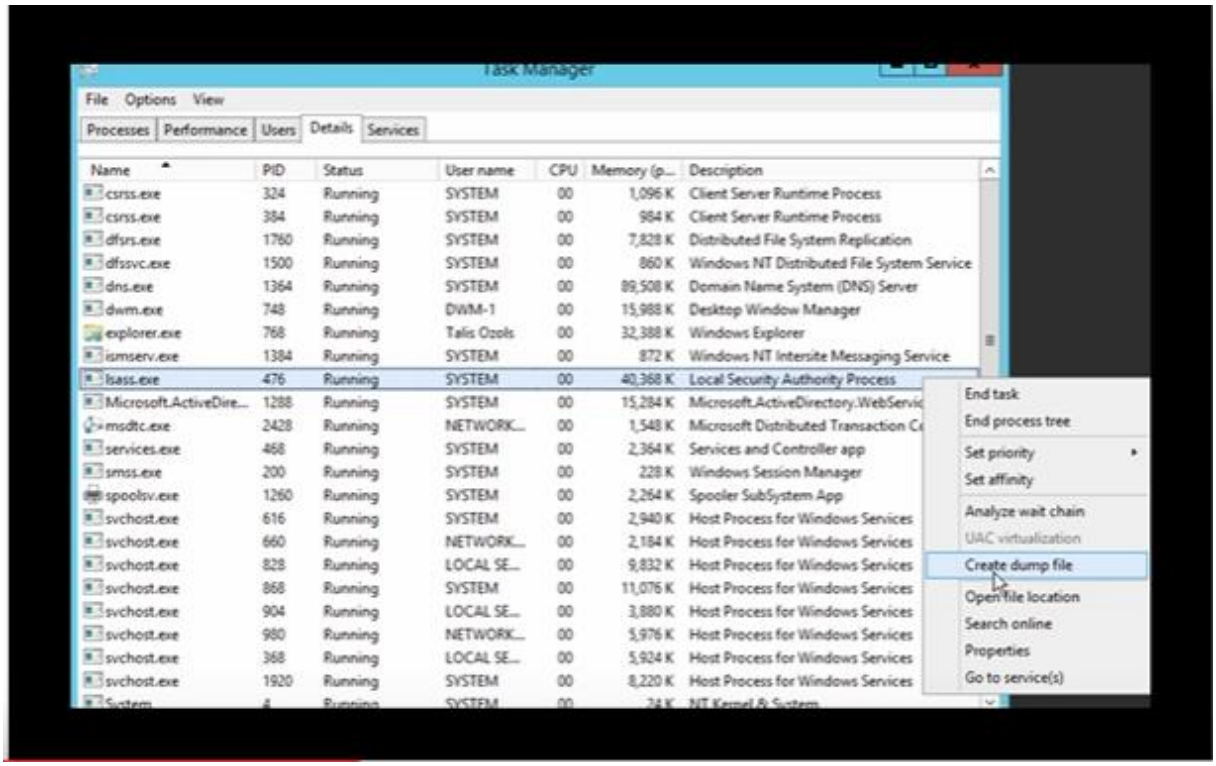
Golden Ticket saldırısı etki alanı denetleyicisine(DC) erişim sağlandıktan sonra gerçekleştirilebilen bir saldırıdır.Saldırganların etki alanı denetleyicisinde KRGBT(ve tüm kullanıcıların)parolalarının alınabileceği yetkiye sahip olunması kritk bir yönetim zafiyetidir.
Korunma Yöntemleri
KRBGT şifresini düzenli olarak değiştirin
KRBGT parola hashine erişebilecek hesap sayısını en aza indirin
Log kayıtları kontrol edilmelidr
Bal küpü nesneleri oluşturulmalıdır

6)LSASS Dump ile Parola Elde Edilmesi

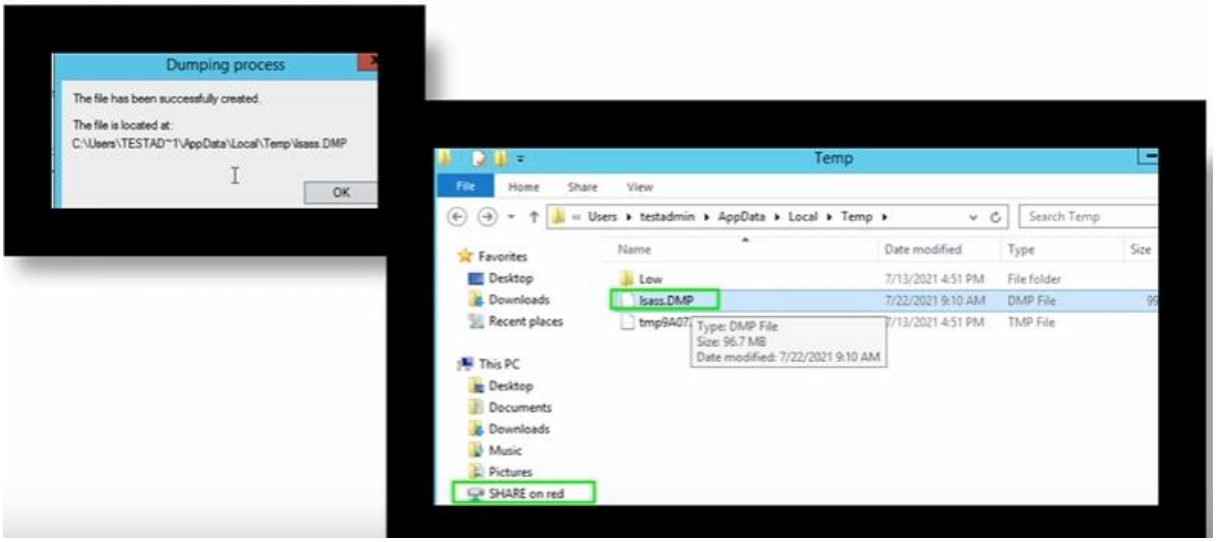
Lsass prosesi Windowsta kullanıcı kimlik doğrulamasını parola değişikliklerini ve güvenlik ilkelerinin uygulamasını yöneten süreçtir.

LSAS Dump saldırılarının temelinde admin veya yetkili biri olmadan sistem üzerinde ısas.exe dosyasını dump ederek bellekten parola bilgisini elde etme yöntemidir.

Öncelikle bağlantı sağladığımızı düşünelim hedef sistem üzerinde görev yöneticisini çalıştırıp lsas.exe dosyasını sağ tıklayıp create dump file diyerek dışa aktarabiliriz



Lsas.dump dosyasını dışarı aktarmış oluruz.Oluşturulan dosya saldırgan dosyasında mimikatz dosyasına kopyalanır.Aynı işlemi mimikatz üzerinden gerçekleştireceğiz.



Mimikatzi çalıştırıyoruz.Bu komut ile dump ettiğimiz dosyayı mimikatze import etmiiş oluyoruz.Bllekte kullanıcı adı ve parola bilgilerini elde etmiş oluyoruz.Görselde Test kullanıcısıısnın

parola bilgileri elde edilmiştir.Bu parolalalrla Brute force uygulayıp hashleri kırabiliriz.